THE SECURITY IMPERATIVE:
DRIVING BUSINESS GROWTH IN THE APP ECONOMY >>

Sponsored by ca technologies

COLEMAN PARKES RESEARCH

Contents

USING THIS INTERACTIVE PDF

Interactivity varies on tablets and smartphones, depending on your PDF reader. You may find interactivity doesn't work when viewing the PDF in email preview mode. We recommend Adobe Acrobat Reader.

HOME (first page) | CONTENTS | BACK one page | FORWARD one page

Executive summary

The application economy has changed the face of IT security. The dividing line between the inside and outside of the enterprise has all but dissolved. The corporate network perimeter has not only moved; it has fragmented. Your new security frontier lies wherever people decide to access your network.

But that's not the only problem. Customers, employees and partners have come to expect seamless, always-on access, on whichever device or platform they're using.

Traditional IT security strategies will no longer work in this complex climate. Organizations must be able to authenticate highly distributed identities from multiple sources, while maintaining a frictionless user experience. There's a delicate balance to strike between robust protection and user satisfaction, and this demands a new, identity-centric approach to security. One that uses context, behavioral analytics and more predictive approaches to deliver a compelling customer experience, while protecting identities and data.

Ultimately, identity-centric security enables you to build the trusted digital relationships with your customers that are your business' greatest asset in the app economy.

With this in mind, CA Technologies commissioned Coleman Parkes Research to survey 1,770 senior business and IT executives, including more than 100 CSOs and CISOs. We asked them about their IT security practices and their adoption of the key elements of identity-centric security.

This enabled us to identify what advanced users of identity-centric security do differently, and what impact their security is having on their businesses.

Our findings make a clear business case for a new model of digital security; one that's in tune with the demands of the app economy, and can drive real improvements that benefit the bottom line.

Identity-centric security enables you to build the trusted digital relationships with your customers that are your business' greatest asset in the app economy.

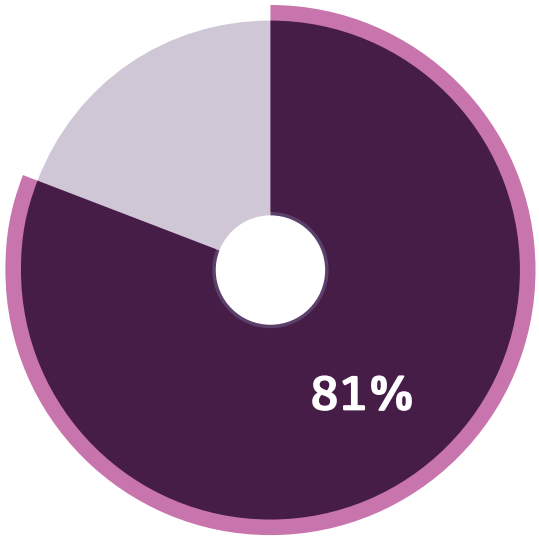
Our analysis revealed that:

- **81%** of enterprises agree that security needs to be frictionless, so as not to burden users with overly onerous security requirements.
- **82%** say identity-centric security is critical to their business, yet **only 25%** can be considered advanced users of identify-centric approaches to security.
- Twice as many advanced users of identity-centric security have seen a reduction in data breaches compared to basic users—**41% versus 21%**.
- **91%** of advanced users of identity-centric security have seen improvement in digital reach; **87%** in customer experience; and **87%** in customer retention.
- Advanced users of identity-centric security are also seeing quantifiable business results:
  - **47%** improvement in new business growth
  - **50%** improvement in employee productivity
  - **45%** improvement in customer satisfaction

"Security is the biggest driver of our digital journey."

Director of technology, US government agency

81% of enterprises agree that security needs to be frictionless, so as not to burden users with overly onerous security requirements.



Introduction: A new frontier

The digital revolution has moved—and continues to move—the IT security goalposts. It has created a multi-channel, multi-platform and multi-device world. A world where your customers, partners and employees are always on, and expect you to be too.

In today's app economy, customers expect fast downloads, quick access, seamless experiences, and robust protection. They'll abandon you if your security slows them down, and may take their business elsewhere if you fail to safeguard their data.

The traditional network perimeter is no more. People access your network whenever and from wherever they choose, and on whichever device or platform they wish. A user identity—not a firewall—is now the frontier in the battle to protect data.

This demands a two-way trusted relationship between the user and the business to succeed.

It's a climate that requires a more identity-centric view of security, which puts the user's identity center stage. Identity-centric security uses context, behavioral analytics and more predictive security approaches to ensure that users are who they claim to be. This will allow them to safely access your company's data on the device of their choice, anywhere, anytime.

"Security is a major obstacle to meeting customers' demands for speed."

IT director, US local government association

People access your network whenever and from wherever they choose, and on whichever device or platform they wish.

However, identity-centric security is more than an effective method of protecting data. Properly executed, it can be a valuable business enabler. It can enable you to deliver new services more quickly. It can also boost customer engagement and loyalty, both of which depend on trust. And in a digital world, security is the primary driver of trust.

"Identity-centric security will become the primary approach to security among telecommunications companies."

Marketing director, European telecoms provider

As part of our research into how enterprises are transforming in the digital era, we examined their efforts to adopt a more identity-centric approach to security. We asked senior business, IT and security executives worldwide about:

- their perceptions of security as an enabler of business opportunities
- the critical KPIs they use to evaluate the impact of IT security, and the results they've seen
- their adoption of the identity-centric security that's required for the app economy
- how more advanced use of identity-centric security impacts business performance

This report summarizes our findings. It looks at how organizations can evolve their IT security to drive increased performance, competitiveness and growth in the app economy.

Identity-centric security is more than an effective method of protecting data. Properly executed, it can be a valuable business enabler.

01. The state of security in the app economy

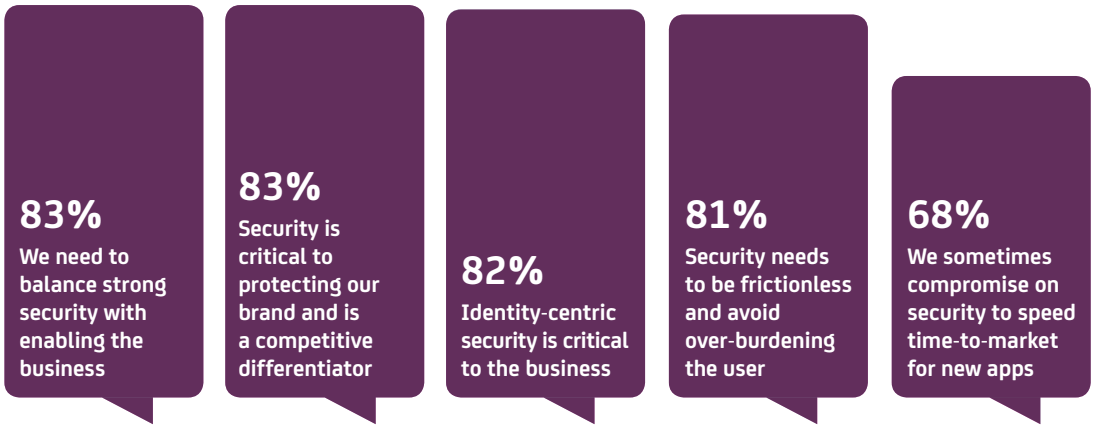
Our research suggests that organizations recognize the role security can play in today's business environment. They remain focused on the traditional goals of security, such as protecting against breaches and ensuring compliance. But at the same time, our survey respondents see security as an opportunity to expand their businesses, and compete more effectively in the app economy.

Over four fifths of survey respondents agree that security can enable new business opportunities; provide a competitive edge; and give employees and customers the fast, convenient and always-on access they've come to expect (see fig. 1).

This is reflected in the key performance indicators (KPIs) being used to assess the impact of IT security. External business performance metrics like digital reach, customer experience and customer satisfaction are as likely—or even more likely—to be used as traditional security measures, such as breaches and compliance audit failures (see fig. 2).

Over four fifths of survey respondents agree that security can enable new business opportunities; provide a competitive edge; and give employees and customers the fast, convenient and always-on access they've come to expect.

FIG. 1 THE APP ECONOMY REQUIRES A NEW ROLE FOR SECURITY AS A BUSINESS ENABLER



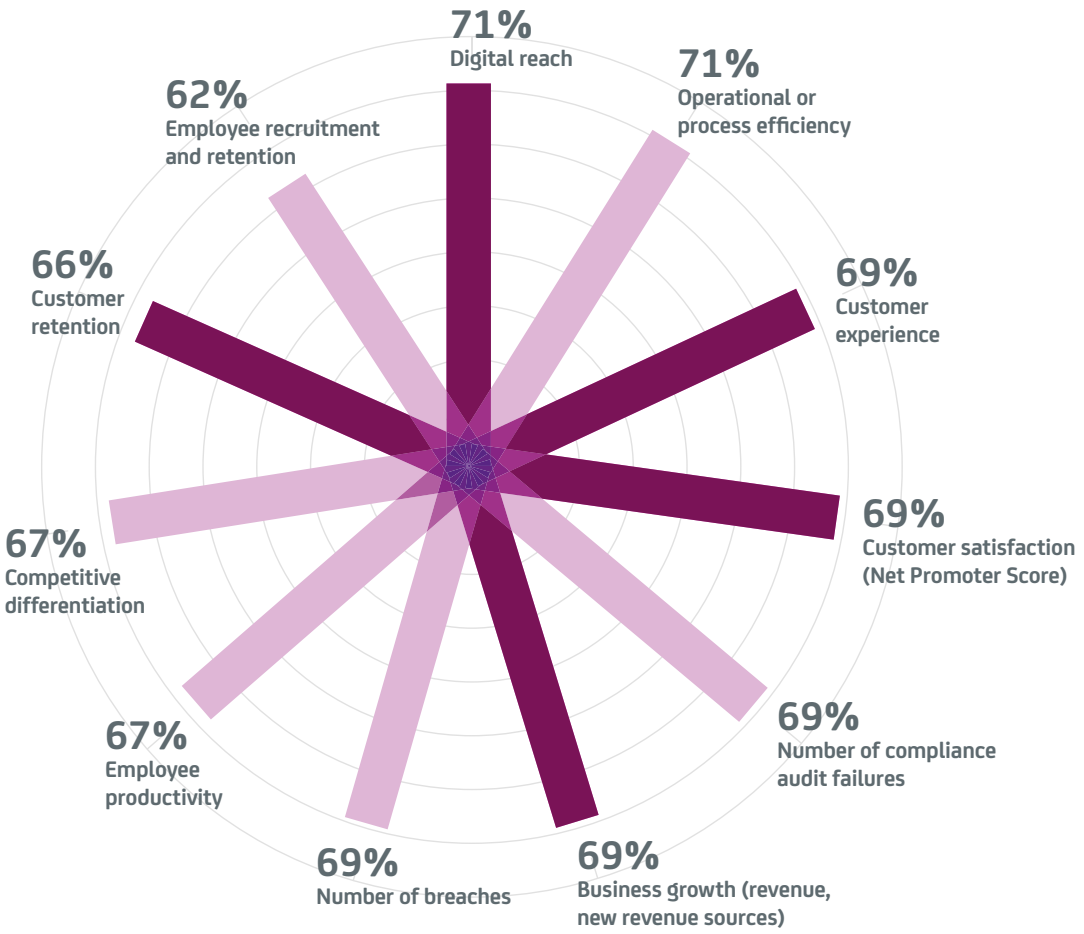
"There is a tug-of-war between robust security on one hand, and customer and employee interfaces on the other."

IT director, US local government association

Businesses clearly see IT security as a critical business enabler, as well as a way to protect data. However, many are cutting corners under the pressures of the app economy. A worrying 68% admit to compromising on security to get apps to market more quickly.

Deprioritizing security in the app economy is a major risk. Managing identities and access across thousands of apps, services and devices demands a much more sophisticated approach to protecting identities and data than has been required in the past.

FIG. 2 EXTERNAL BUSINESS METRICS ARE AMONG THE TOP KPIs USED TO MEASURE THE IMPACT OF IT SECURITY



02. A new approach to security

The challenge in the app economy is to verify highly distributed identities from a wide range of sources, including apps, systems, the cloud and social media platforms.

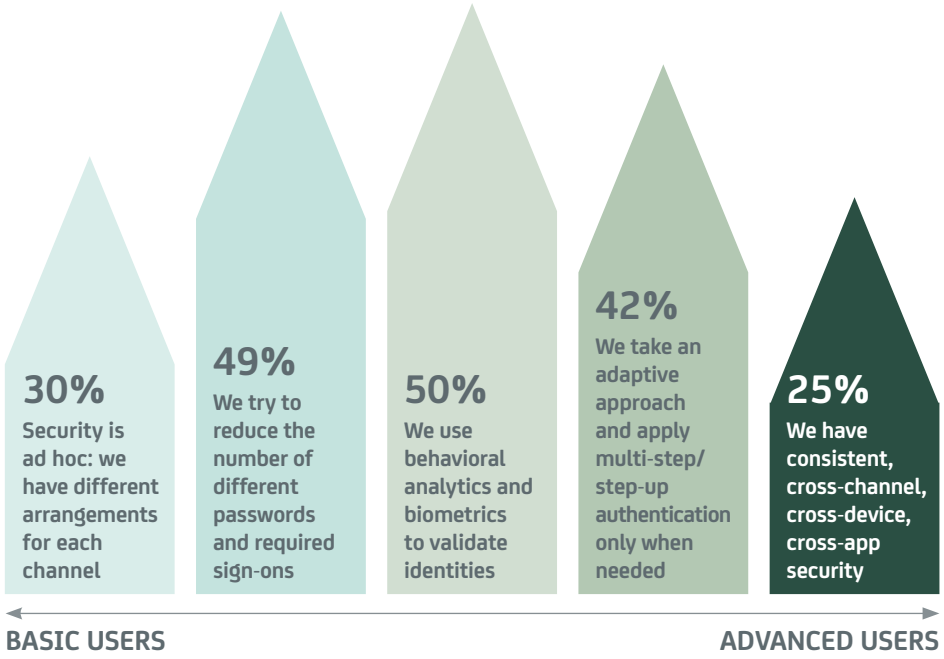
Yet this must be done in a way that's invisible to users. Customers want failsafe security and a frictionless experience. Cumbersome, inconsistent registration and authentication processes will quickly turn them off, and impede efforts to build trusted digital relationships.

Identity-centric security is an approach that helps ensure your security practices don't impinge on the overall user experience. It also requires you to adopt more adaptive IAM (identity and access management) controls; and to take a more proactive and predictive approach to preventing and detecting data breaches.

We created a maturity model to assess organizations' adoption and current usage of three key elements of identity-centric security:

1. **Customer experience** (see fig. 3). Consistent, cross-channel approaches to security, using behavioral analytics and adaptive techniques, will result in less intrusive security. Just a quarter of enterprises use consistent, cross-channel, cross-device and cross-app security to maintain a high quality user experience. A minority (42%) take an adaptive approach, while half are using behavioral analytics.

FIG. 3 CONSISTENT, CROSS-CHANNEL APPROACHES TO SECURITY DRIVE CUSTOMER EXPERIENCE, BUT FEW HAVE ACHIEVED IT



"Security has to become more user-friendly, without sacrificing its robustness. The key is to ensure you can identify whether a user is a customer, employee or hacker; safeguard customer and employee data; and make sure that transactions aren't impaired."

VP of technology & compliance, US banking organization

2. **Identity and access management** (see fig. 4). Identity-centric security also requires a more adaptive approach to IAM controls. Almost 70% have centralized and automated IAM controls; but only one in ten can adapt them in response to risks.

"Identity and access management will be the main security concern in the future."

Marketing director, European telecoms provider

3. **Breach detection** (see fig. 5): Proactive and predictive processes can greatly enhance an organization's ability to detect and prevent data breaches. Yet only 37% use analytics to proactively detect and prevent data breaches; and less than half that number (16%) can predict the risk of breaches before they occur.

After asking participants questions about these three elements of identity-centric security, we scored their responses. Based on the results, we categorized their organizations as advanced, basic or limited users of identity-centric security.

We found only 25% of enterprises to be advanced users. By far the largest proportion (64%) are basic users, while just over one in ten (11%) have limited, if any, identity-centric capabilities.

FIG. 4 ADAPTIVE IDENTITY AND ACCESS MANAGEMENT CONTROLS IMPROVE IDENTITY-CENTRIC SECURITY, BUT FEW HAVE ADOPTED THEM

20% Controls are predominantly manual

69% Controls are predominantly centralized and automated

11% Controls are adaptive based on risk

BASIC USERS — ADVANCED USERS

FIG. 5 PROACTIVE AND PREDICTIVE ANALYTICS HELP TO DETECT AND PREVENT DATA BREACHES, BUT FEW ARE USING THEM

13% Occasional review of activity reporting only

34% Some analysis with smart reporting and alerts

37% Proactive: in depth analysis with real-time response to events and incidents

16% Predictive: can anticipate risk before a breach occurs

BASIC USERS — ADVANCED USERS

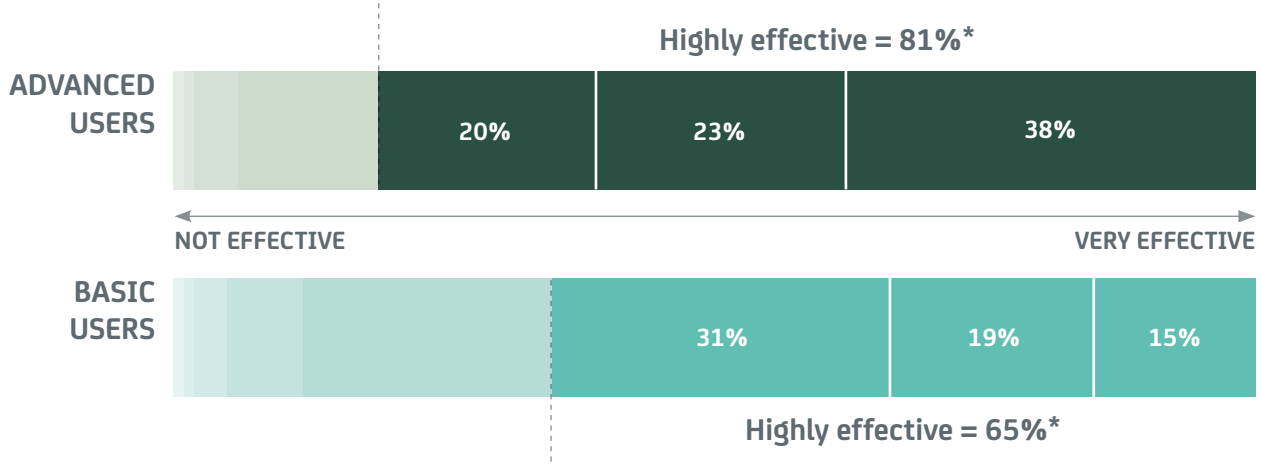
03. The significant business impact of identity-centric security

The next stage of our analysis was to see if there's a correlation between mature use of identity-centric security and business results. To do this, we compared the business performance of advanced and basic users.

Our analysis found that advanced users of identity-centric security are far more likely to believe their security differentiates them from the competition. Some 81% say their security strategy does this, compared to 65% of basic users (see fig. 6).

Advanced users also make a much higher priority of all of the security objectives we asked about (see page 8). Most significantly, they're much more likely than basic users to leverage security to enable new business initiatives and relationships (55% versus 34%).

FIG. 6 ADVANCED IDENTITY-CENTRIC SECURITY ENHANCES COMPETITIVE DIFFERENTIATION

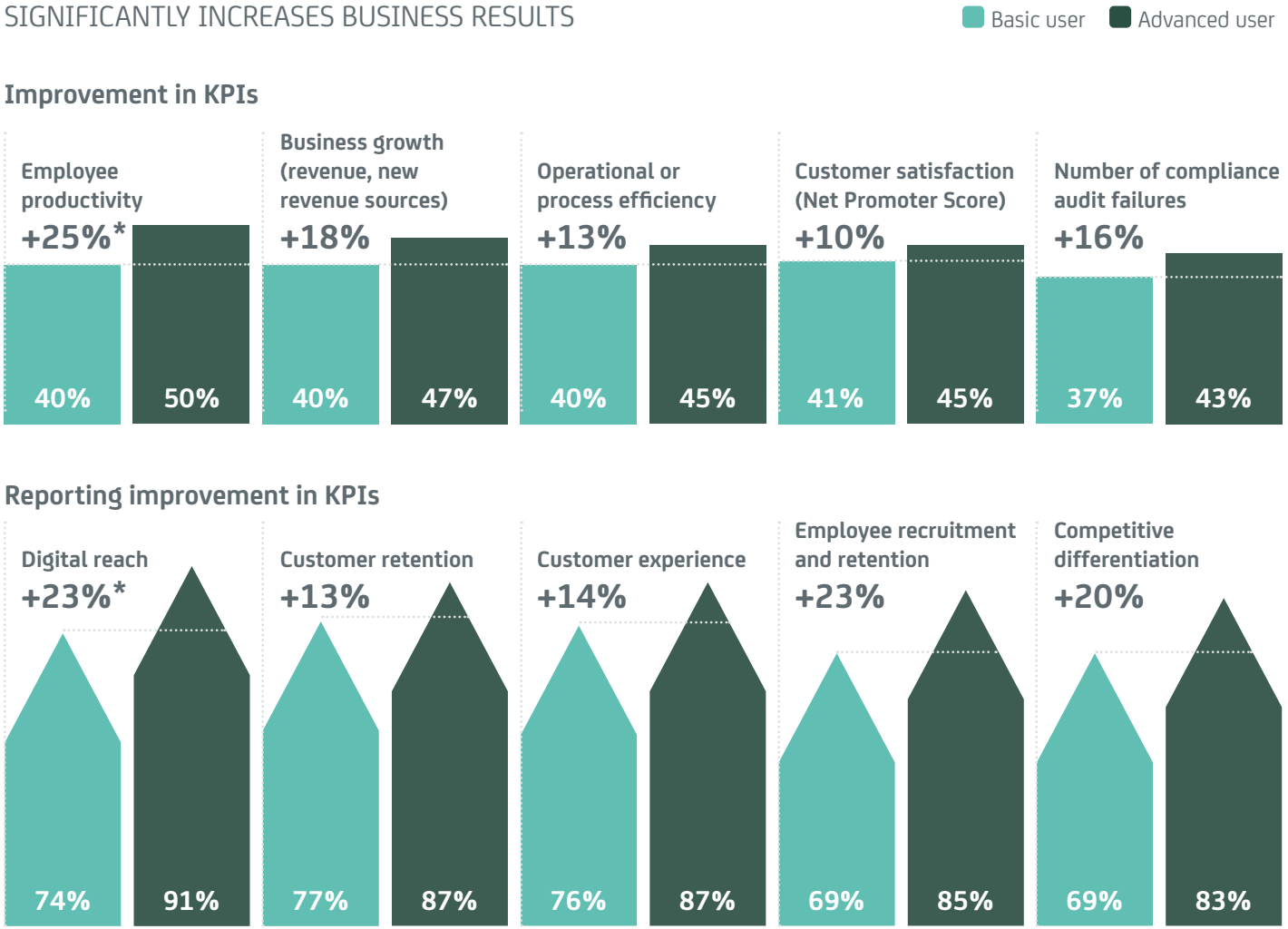


* % Top 3 ranks out of 10, where 10 is very effective and 1 is not effective

A similar picture emerged when we looked at the impact of IT security on the KPIs used to evaluate it. Advanced users of identity-centric security attribute greater improvements in all of the business and security measures we asked about.

The differentials between advanced and basic users range from 10% to as much as 25% (see fig. 7). For instance, 87% of advanced users report significant improvement in customer experience, versus 76% of basic users. And an even bigger impact can be seen in employee retention and recruitment: 85% of advanced users report an improvement, compared to 69% of basic users.

FIG. 7 MOVING FROM BASIC TO ADVANCED IDENTITY-CENTRIC SECURITY SIGNIFICANTLY INCREASES BUSINESS RESULTS



* % improvement in KPIs moving from basic to advanced user

In terms of data protection, while about a third of all users are still seeing an increase in security breaches, it is significant that advanced users are almost twice as likely as basic users to have reduced the number of data breaches they encounter. Two fifths (41%) of advanced users managed this in the past year, despite an increasingly challenging security climate. This compares to less than a quarter (21%) of basic users (see fig. 8).

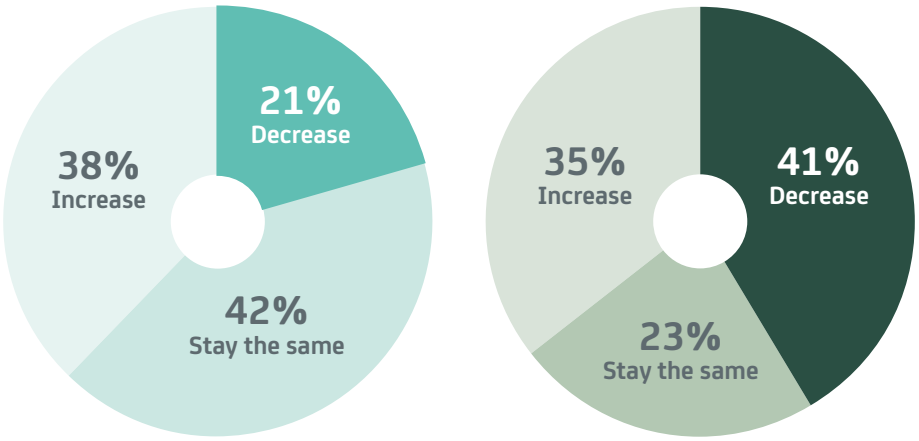
Digital Transformation Business Impact Scorecard

We also assessed the impact of identity-centric security on respondents' digital transformation efforts.

To do this, we used the Digital Transformation Business Impact Scorecard, which we created as part of our research into enterprises' digital transformation efforts. The scorecard assesses the overall effect of organizations' digital initiatives, based on 14 business KPIs that are essential to successful transformation.

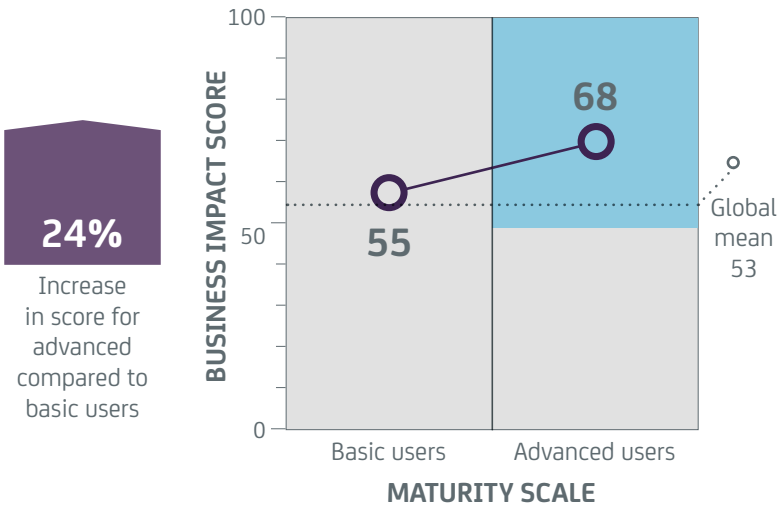
We compared the scorecard results for advanced and basic users of identity-centric security. The average score for advanced users was 68 out of 100, compared to just 55 for basic users: an improvement of 24% (see fig. 9).

FIG. 8 MOVING FROM BASIC TO ADVANCED IDENTITY-CENTRIC SECURITY REDUCES DATA BREACHES



Percentage of enterprises reporting data breaches have increased, stayed the same, or decreased
(Percents do not sum to 100 due to rounding)

FIG. 9 ADVANCED USE OF IDENTITY-CENTRIC SECURITY INCREASES DIGITAL TRANSFORMATION BUSINESS RESULTS



04. Lessons from advanced users of identity-centric security

The message is clear: mature adopters of identity-centric security are driving greater business benefits across the board. So what do they do differently that makes their security so much more effective?

Firstly, they take IT security more seriously: 81% are investing more in breach prevention, compared to 55% of basic users. And they're less likely to cut corners: 58% of advanced users compromise on security to get their apps to market faster, compared to 70% of basic users.

They also are more likely to make use of what's known as 'DevSecOps'. A majority of advanced users of identity-centric security (54%) use this practice, compared to 33% of basic users.

DevSecOps is crucial in the app economy. When your business depends on digital technology, you can't bolt security onto your apps as an afterthought. Similar to DevOps, which integrates IT operations earlier into the software development cycle, DevSecOps brings security into the development process sooner. This ensures that security is built in to your digital applications from the outset.

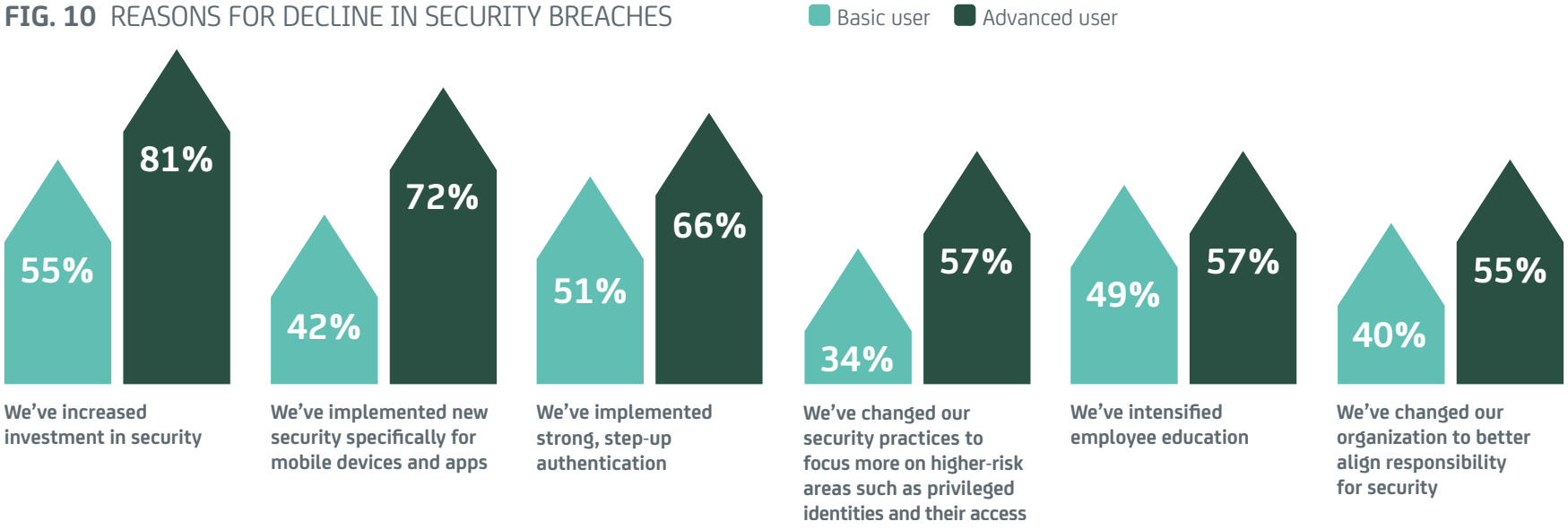
Finally, advanced users do more to align their approach to breach prevention with the realities of the app economy (see fig. 10).

They're significantly more likely to implement dedicated security for mobile devices and apps (72% vs 42%); reconfigure security practices to protect high-risk areas like privileged identities (57% vs 34%); deploy strong, step-up authentication (66% vs 51%); and restructure the business to strengthen responsibility for security (55% vs 40%).

"Our greatest security headache is the remote access that everyone now has. Authentication has been the focus of our IT security over the last two years."

R&D director, US pharmaceutical manufacturer

FIG. 10 REASONS FOR DECLINE IN SECURITY BREACHES



05. Effective identity-centric security: A roadmap

Our study makes a strong business case for embracing identity-centric approaches to security. But how do you get started? How do you make it work for your business? And how do you ensure that it improves performance and drives growth?

In our experience, the following actions are crucial to the successful implementation of identity-centric security:

1. **Make identity your perimeter.** Users are now your security boundary, and they're accessing your network from everywhere, at all times. You need to know that they are who they claim to be, and that they can only access the information and services they should. This means considering risk-based authentication combined with analytics-based approaches to assessing identities.
2. **Treat security as a business enabler.** In the app economy, security is there not just to reduce risk; it also enables new business growth. Our research shows that an identity-centric approach can drive a range of benefits that improve the bottom line. So build business performance indicators into your security evaluation framework.
3. **Focus on creating trusted digital relationships**. The greatest assets you have are the digital relationships you build with your individual customers. They need to trust that you understand their needs when interacting with your company, and are protecting their identity and data as seamlessly as possible.
4. **Protect experiences, not just data**. Security needs to be robust, but also frictionless. Customers want streamlined interactions and quality experiences; any disruption will only put them off. This means offering single sign-on access; self-service capabilities; and consistent but flexible authentication mechanisms as people move among apps and devices.
5. **Take an adaptive approach to IAM**. Our research shows that mature users of identity-centric security have IAM controls that can be readily adapted in response to risks, offering a significantly improved user experience.
6. **Be proactive and predictive**. Advanced analytics can help you to proactively fend off security risks, instead of being constantly in firefighting mode. And they can take your security a stage further: they can help you sense, react and adapt security processes to address the risk of breaches before they occur.
7. **Don't compromise security for speed**. The app economy has increased the pressure to release new apps quickly. But it's more important than ever to ensure that security is built in right from the start, and not compromised at the end. Consider using a DevSecOps approach to make sure that all security considerations are addressed early in the development process.

Further information

Research methodology

CA Technologies commissioned Coleman Parkes Research to interview executives about the extent and impact of their organizations' digital transformation activity.

We surveyed 1,770 senior business and IT decision-makers (including 106 CSOs/CISOs) at large enterprises in 21 countries across the Americas, EMEA and Asia-Pacific Japan (APJ) regions. Organizations surveyed had annual revenues of more than US$1 billion (or US$0.5 billion in some smaller economies).

Countries surveyed were:

Americas	**EMEA**	**APJ**
Brazil	France	Australia
USA	Germany	China
	Italy	Hong Kong
	Netherlands	India
	South Africa	Indonesia
	Spain	Japan
	Sweden	Korea
	Switzerland	Malaysia
	UK	Singapore
		Thailand

Sectors surveyed were:

- Automotive
- Banking and financial services
- Energy and utilities
- Healthcare
- Manufacturing
- Media and entertainment
- National public sector
- Retail
- Telecommunications
- Transportation and logistics

The research and analysis were conducted in May and June 2016.

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. www.ca.com

About Coleman Parkes Research

Coleman Parkes Research specializes in recruiting and interviewing senior-level respondents across multiple global markets, vertical sectors and functional areas for a wide range of clients. From thought leadership research for PR and marketing campaigns, to analyzing win/loss opportunities, testing product messages and conducting in-depth senior executive interviews, we do it all. Coleman Parkes Research works collaboratively with clients to formulate proven strategies that generate market insight based on individual requirements and key hypotheses. colemanparkes.com/

About Grist

Editorial and creative services. Grist is an award-winning B2B thought leadership and content marketing agency with the editorial heritage of The Economist and Financial Times in our DNA and a clear view of the digital future. www.gristonline.com