TREND STUDY: CYBERSECURITY
EXECUTIVE SUMMARY

Identity and Access Management in the Digital Age

Paul Fisher, Research Director

May 2016

Premium Sponsor —— Gold Sponsors —— In partnership with

KPMG Computacenter CYBERARK kuppingercole ANALYSTS vmware SailPoint

PAC
A CXP GROUP COMPANY

TABLE OF CONTENTS

TABLE OF FIGURES

PREFACE

Many enterprises are scrambling to transform their businesses to take advantage of the new digital economy. This transformation journey may often introduce risks, which if not carefully managed, can expose the weaker links in their cybersecurity protection.

The issue can be further complicated by the fact that existing platforms and technologies, including Identity and Access Management (IAM) solutions, which deliver key business processes today were not built to address digital economy imperatives like the Internet of Things (IoT), hybrid cloud, social identities and the obfuscation of the identity perimeter.

For cybersecurity and IAM specialists these are stimulating times because, as they grapple to understand the many vectors of insider risk, the digital transformation opportunity comes knocking hard on the door.

Caught up in this vortex of change, clients are faced with more questions than answers:

- What is the span of the identity perimeter?
- How far apart are the principles of managing enterprise and customer identities (really)?
- Is a single view across internal and external identities possible?
- IAM as a digital transformation critical service – how does it impact delivery, training and adoption?

In association with PAC and KuppingerCole, we have attempted to chart the role of IAM in digital transformation through this study. We hope that this report will engender a greater appreciation of the role of IAM in digital transformation and ultimately help with comprehending IAM's journey into the heart of business transformation.

Manoj Kumar
Principal Advisor,
Cyber Security,
KPMG in the UK

John Hermans
Cyber Security Lead,
Europe, Middle East and Asia
KPMG in the Netherlands

The infographic for this study is available at https://www.pac-online.com/trend-study-identity-and-access-management-digital-age.

To download the full study, please visit our sponsors' websites.

Identity and Access Management in the Digital Age

Paul Fisher
Research Director, PAC UK
May 2016

INTRODUCTION

Keeping enterprises secure and ensuring that only the right people can access data and systems has long been the role of the tens of thousands of Identity and Access Management (IAM) systems installed across Europe.

Traditionally, such solutions have been configured to manage personal identities of employees and have scaled to manage the shift to mobile working, and multiple endpoints.

But today a new challenge is emerging as European businesses, across all verticals, are looking to embrace digital transformation to improve competitiveness, gain efficiencies or get closer to customers and supply chain.

More than just a buzzword, digital transformation is really happening across Europe - as the results of our study show.

But digital transformation will have an impact on existing technologies and processes too. At the heart of keeping the organization secure as it transforms will be secure identities.

However identities in the digital age are likely to multiply exponentially and present themselves in different and more challenging forms. For the first time, businesses are contemplating the role of consumer identities in the enterprise, how they can be managed and how they can be secured. The public sector is contemplating how digital identities can be used to transform public services.

This challenge will, in a very short space of time, be one that senior security and information chiefs across Europe will need to address – if they are not doing so already. They will need to look at how IAM solutions will assist them in managing the identity needs of the digital business.

We believe this study provides valuable insights into how IT decision makers across Europe are preparing to face the new cyber security challenges of identity and access management systems in a changing business environment.

Businesses are contemplating the role of consumer identities in the enterprise.

KEY FINDINGS

The findings shows a significant awareness among senior IT decision makers of the need for IAM solutions that can function securely, while fulfilling the challenges and opportunities of the digital age.

Senior security and information chiefs from banking, insurance, manufacturing, retail, services, telecoms, transport and the public sector across major European territories revealed a concern that the onset of digital transformation could only achieve its benefits if security is baked in.

When questioned on what were the primary goals of their digital transformation strategies, 48% of respondents said threat or breach mitigation was very important.

Shadow IT is emerging as a serious threat to secure IAM deployment in the digital age.

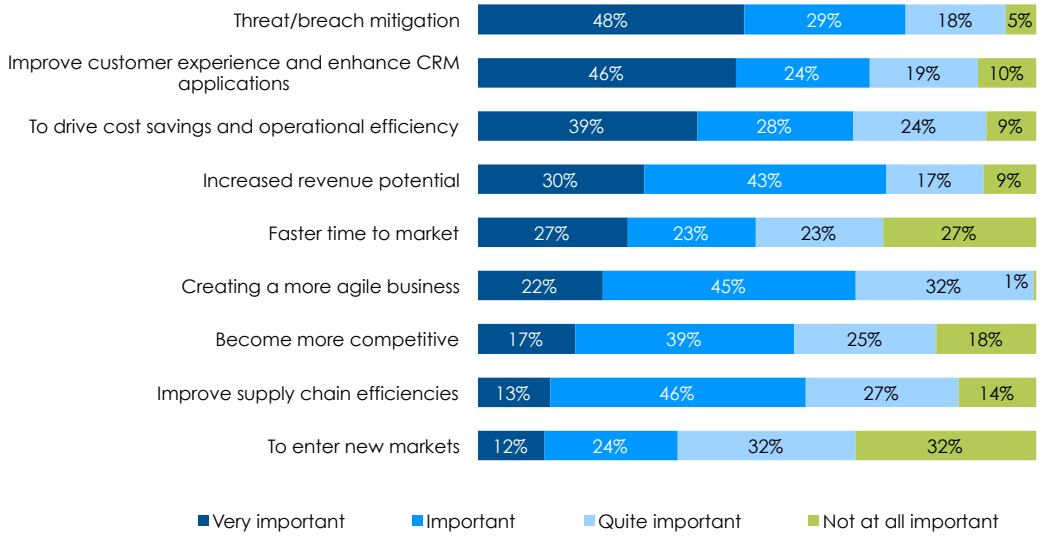

Fig. 1: Importance of individual goals of digital transformation strategies

This was placed higher than improving customer experience or driving costs savings and efficiencies – both expected enterprise priorities for the businesses surveyed.

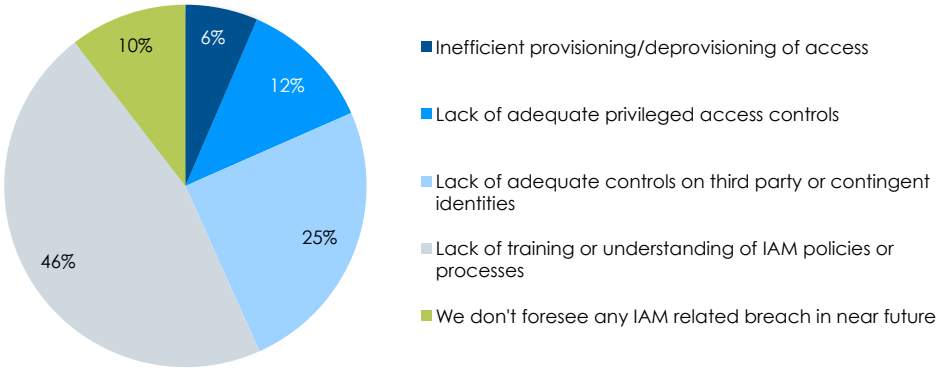

Fig. 2: Main cause of next IAM-related breach

Of the respondents, 46% said that they believed the lack of training or understanding of IAM policies or processes would be the main cause of the next IAM related breach.

Meanwhile, shadow IT is emerging as a serious threat to creating a secure IAM solution as companies digitally transform, with 43% saying it was challenging, and 22% very challenging.

Other highlights of the study:

- 92% of respondents will maintain or increase their IAM investment in the next three years
- 65% of respondents see consumer identities and applications as a factor in their next IAM investment
- 57% of respondents are considering adopting a solution at least partly managed by a Managed Security Services Provider (MSSP) for their next IAM investment

92%

of organizations in Europe will maintain or increase their IAM investment in the next three years.

77%

of businesses in Europe are undergoing digital transformation

IAM AND THE DIGITAL AGE

Digital transformation is changing business models, technology strategies, and partnerships in order to make businesses ready for the opportunities and challenges of the digital economy.

According to our study, it's a process well underway across Europe with some 77% of respondents saying that their organization has already implemented an enterprise wide transformation strategy, or already changing some enterprise operations.

This is a significant number and is likely to increase in the next three years as more companies realize that to compete effectively in a digital market, they need to go digital themselves.

Even those sectors once thought resistant to digital change, like insurance or manufacturing, are accelerating their programs, according to our results.

This could mean embracing digital outside of the traditional boundaries of the business, getting closer to customers through social media or making use of omni-channel trading models, particularly in the retail sector.

SECURING THE DIGITAL BUSINESS WITH IAM

When we asked respondents what were the important goals of their organization's digital transformation we got some surprising, and some not so surprising results.

However it's significant that 48% of respondents thought threat or breach mitigation was a very important prerequisite for digital transformation.

Significant because if they are influential enough in their organizations there is a greater chance that transformation will be secured from the outset.

While it was expected that security would be well understood as a major challenge by our sample, they are not working in security bunkers either, blinkered to the needs of the business. Beyond security, the strategic goals of business transformation also figure highly in the responses.

These include improving customer experience, driving operational efficiency and increased revenue potential.

48%

of senior IT leaders in Europe think threat or breach mitigation is a very important component of digital transformation.

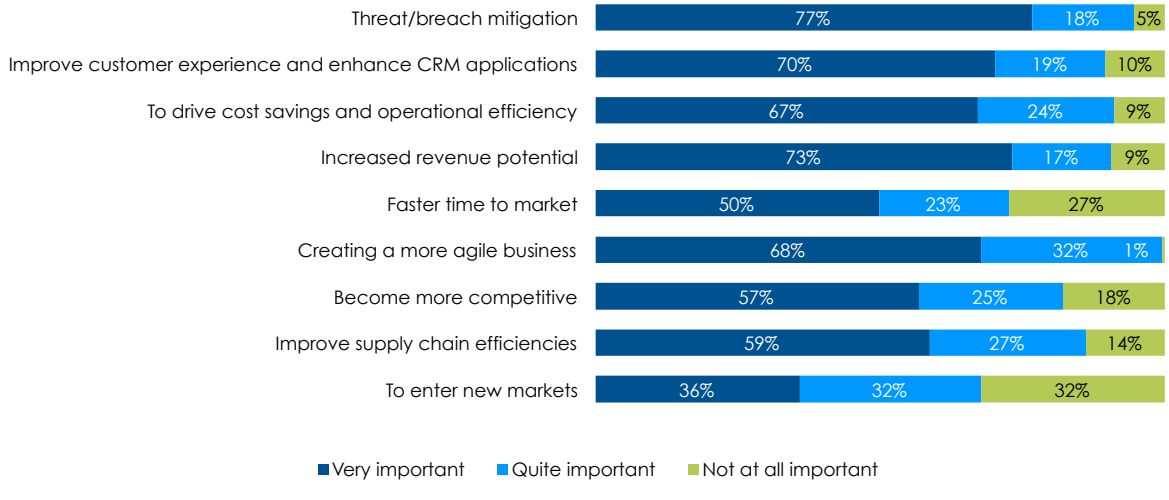

Fig. 3: Importance of individual goals of digital transformation strategies

THREAT VECTORS FOR IAM

Digital will increase threats across a number of vectors including mobile, cloud and shadow IT.

MOBILE COMPUTING

Mobile computing will impact on the security of identities as businesses transform, and its growth is across all sectors.

THE CLOUD

The shift to the cloud is in line with general expectations with all sectors expecting an increase in corporate systems sitting in the cloud in three years time.

SHADOW IT

And in the digital age, one area where people are already "failing" is in the deployment of Shadow IT, which remains a controversial topic in IT circles.

65%

of senior information security decision makers in Europe see Shadow IT as a challenge to creating a secure IAM solution.

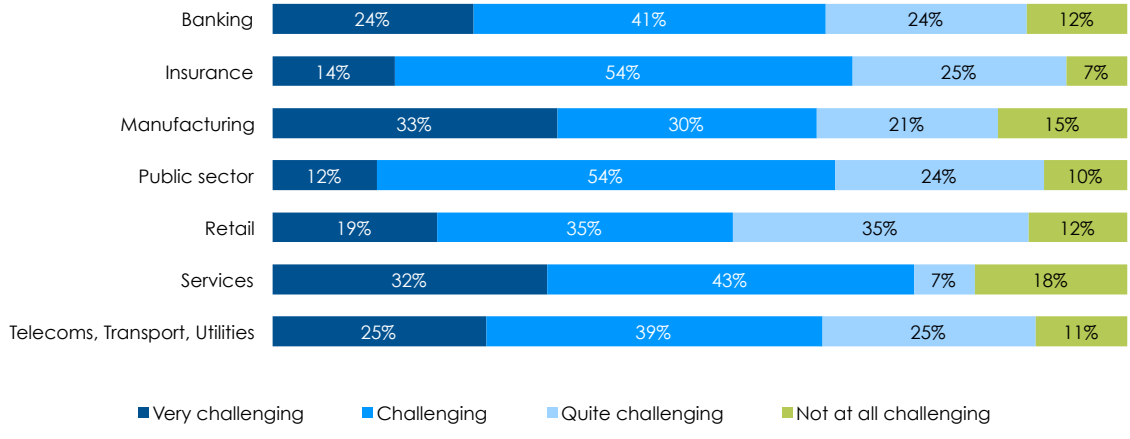

Fig. 4: How challenging is Shadow IT in creating a secure IAM solution for digital transformation within the next 2-3 years?

RISKS AND REWARDS OF IAM

We live in an age where cyber attacks are constant and no company or organization is immune from breach. And even the best IAM solutions can be breached if rules are broken, or if operational changes take place that are not sanctioned by IT. Increasingly security at European businesses is threatened by the growth in shadow IT.

We wanted to know what our sample thought the main causes of the next IAM related breach could be. For those in the enterprise who do not believe in the power of security awareness training the results may serve as a wake up call.

For 46% of all respondents across all sectors believed that lack of training or understanding of IAM policies or processes could lead to an IAM related breach. This is a situation that could potentially get worse as the complexities of digital transformation take hold.

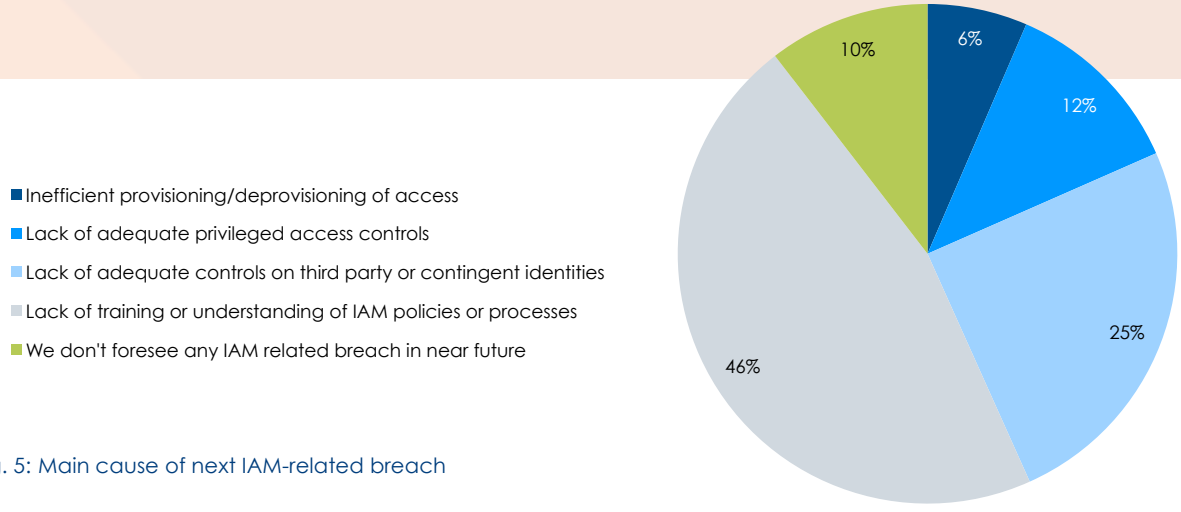

Fig. 5: Main cause of next IAM-related breach

.

CONCLUSION

Our study has revealed an encouraging awareness of the need for digital transformation of their business by our representative sample of senior information and security executives across Europe.

We are seeing too that those verticals seemingly resistant to digital transformation, such as insurance, are starting to shift as market conditions change and challengers emerge. This will mean that security across all sectors will at some point need to adapt to digital transformation, and probably earlier than later.

As new levels of access are likely to form part of digital transformation, the need for a secure and enhanced IAM solution must be factored in from the start.

In a business world increasingly under scrutiny from regulators, a public worried about data privacy, and shareholders concerned about the damage breaches can do to a business, risk and compliance must also be factored into IAM decisions in the digital age.

Identity and access management will move center stage as the main defense against cyber attacks in the digital age, even as businesses move to more intelligence based approach to cyber security and threat management of other vulnerabilities.

APPENDIX

RESEARCH METHODOLOGY

PAC conducted the survey during March 2016. After qualifying, 202 senior information security leaders from across Europe completed our survey. The executives are employed in banking, insurance, manufacturing, retail, services, telecoms, transport and the public sector and are based in the Benelux and Nordic regions, Switzerland, France, Germany and the UK.

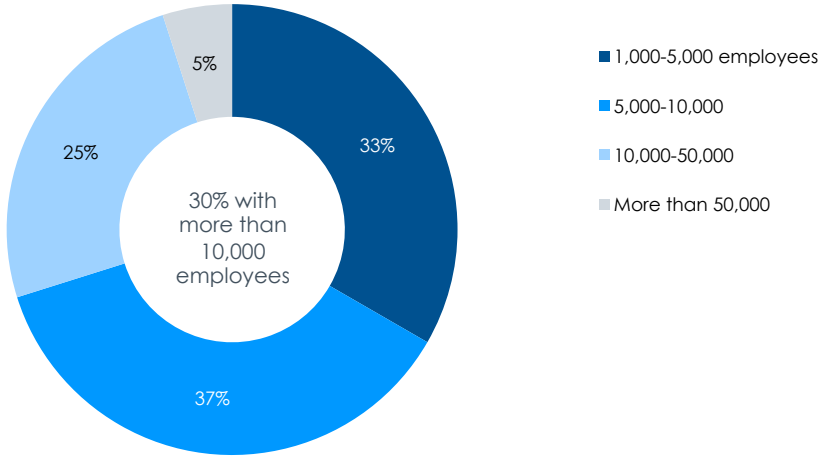

Fig. 6: How many employees work at your company?

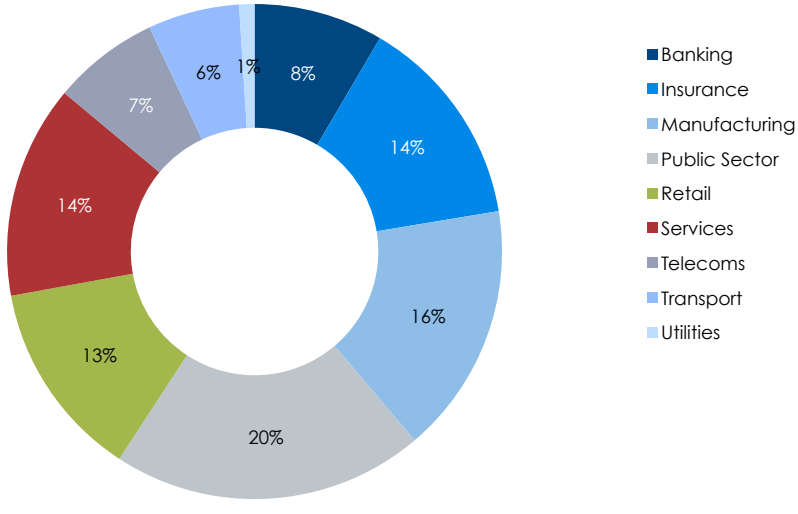

Fig. 7: What is the main activity of your company?

ABOUT KPMG

Today, cyber attacks have become a business reality. Technological advances and changing working practices have created additional opportunities for cyber criminals and hacktivists. Organizations are in a position where they're 'losing control.'

Passwords are being shared; there are silo solutions per application or platform which give rise to countless authentication methods and password regimens; authorizations are multi-layered and duties are no longer clearly segregated; there is a lack of insight into the authorizations granted by the management; the helpdesk costs to change passwords, demonstrate compliance with access governance, protect high-privileged accounts, provide rapid provisioning and de-provisioning and authorizations are high.

The list of weak points are endless.

To address these issues many organizations have projects underway to improve user management, access governance, privileged access management, federation services, Role Based Access Control and provisioning: the ingredients of Identity and Access Management (IAM).

KPMG's Global Cyber Security practice offers many years of experience and extensive expertise in all aspects of IAM:

- An in-depth **understanding** of current and future IAM trends impacting business across multiple sectors
- **Expert knowledge** on compliance laws, business, privacy and regulatory risks
- **Strengths in IAM strategy assessments, program advisory, project management and implementation** across a broad range of IAM tools.
- **Extensive capabilities** in security assessment and certification; security architecture development and implementation; security and technology governance; IT infrastructure and controls; and operations and project risk management

About the KPMG Global Cyber Security Practice

KPMG's 1,200+ network of cyber security professionals' work with companies around the globe to help them safeguard their entire organization. By addressing people, privacy, information governance and business resilience, we help our clients to implement a firm-wide approach to doing business in the digital world. We give leadership a new perspective to help them to take control of cyber risk in a unique and positive way, and empower them to grow, transform and innovate their business.

For more information visit the KPMG Cyber Security website.

Contact:

John Hermans
Cyber Security Lead,
Europe Middle East & Asia
KPMG in The Netherlands

hermans.john@kpmg.nl

Prasad Jayaraman
Global Lead, Identity &
Access Management
KPMG in the US

prasadjayaraman@kpmg.com

Manoj Kumar
Principal Advisor,
Cyber Security
KPMG in the UK

manoj.kumar@kpmg.co.uk

www.kpmg.com

ABOUT COMPUTACENTER

Computacenter is Europe's leading independent provider of IT infrastructure services, enabling users and their business. We advise organizations on IT strategy, implement the most appropriate technology, optimize its performance, and manage our customers' infrastructures. In doing this we help CIOs and IT departments in enterprise and corporate organizations maximize productivity and the business value of IT for internal and external users.

Computacenter provides user support, the best devices, and secure provision of applications and data to support individual working styles and improve collaboration. To achieve this, we assist with consulting as well as the implementation and operation of networks and datacenter infrastructures on or off customers' premises and in the cloud.

Rooted in core European countries Computacenter combines global reach with local expertise. We operate infrastructure Operations Centers and Group Service Desks across Europe, South Africa and Asia from which our employees provide user support in 18 languages. Customers with global requirements are served through an extensive international partner network, which mirrors the requirements of our European-headquartered client base.

In 2014, Computacenter had around 13,000 employees and achieved a revenue of approximately GBP 3.1 billion.

Contact:

Shahriar Saravandi-Rad
Lead Consultant
Consulting Services –
Secure Information

+49 (162) 1312563

Shahriar.Saravandi-Rad@computacenter.com

Computacenter AG & Co oHG

ABOUT CYBERARK

CyberArk is the only security company laser-focused on striking down targeted cyber threats, those that make their way inside to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk is trusted by the world's leading companies — more than 40% of the Fortune 100 — to protect their highest-value information assets, infrastructure and applications.

For over a decade CyberArk has led the market in securing enterprises against cyber attacks that take cover behind insider privileges and attack critical enterprise assets. Today, only CyberArk is delivering a new category of targeted security solutions that help leaders stop reacting to cyber threats and get ahead of them, preventing attack escalation before irreparable business harm is done.

At a time when auditors and regulators are recognizing that privileged accounts are the fast track for cyber attacks and demanding stronger protection, CyberArk's security solutions master high-stakes compliance and audit requirements while arming businesses to protect what matters most.

With offices and authorized partners worldwide, CyberArk is a vital security partner to 2,500 global businesses, including:

- More than 40% of the Fortune 100
- 17 of the world's top 20 banks
- 20% of the Global 2000
- 8 of the world's top 16 pharmaceutical companies
- 75 of the leading energy companies

CyberArk has offices in the U.S., Israel, U.K., France, Germany, Netherlands and Singapore and serves customers in more than 65 countries.

Find us on Linked: www.linkedin.com/company/cyber-ark-software

Follow us on Twitter: @CyberArk

Contact:

Amanda Coles
EMEA Marketing Director

M: +44 (0) 7943 046139

amanda.coles@cyberark.com

www.cyberark.com

ABOUT SAILPOINT

As the fastest-growing, independent identity and access management (IAM) provider, SailPoint helps hundreds of global organizations securely and effectively deliver and manage user access from any device to data and applications residing in the datacenter, on mobile devices, and in the cloud. The company's innovative product portfolio offers customers an integrated set of core services including identity governance, provisioning, and access management delivered on-premises or from the cloud (IAM-as-a-service). For more information, visit www.sailpoint.com.

What We Do

Today, SailPoint helps organizations around the world securely and effectively deliver and manage user access from any device to data and applications in the datacenter, on mobile devices, and in the cloud. SailPoint's products allow companies to mitigate the risks associated with access by delivering:

- **Identity Governance** – streamline compliance processes and improve audit performance through automated access certifications, policy management and audit reporting.
- **Provisioning** – deliver access to business users while reducing costs and tightening security with self-service access request and automated provisioning.
- **Password Management** – strengthen password policies and reduce IT and helpdesk costs with intuitive self-service password management.
- **Access Management** – increase end user productivity with convenient single sign-on (SSO) to cloud and web applications—from any device, anywhere in the world.
- **Identity Intelligence** – get the big picture with centralized visibility to access privileges across the organization and the right information to enable effective business decisions.

Contact:

Reuben Braham
Director of Marketing
EMEA & APAC

reuben.braham@sailpoint.com

Jon Burghart
VP EMEA, SailPoint

jon.burghart@sailpoint.com

Peter Wilson
UK Channel &
Alliance Manager

peter.wilson@sailpoint.com

ABOUT VMWARE

VMware is a leader in cloud infrastructure and business mobility. Built on VMware's industry-leading virtualization technology, our solutions deliver a brave new model of IT that is fluid, instant and more secure. Customers can innovate faster by rapidly developing, automatically delivering and more safely consuming any application.

With 2015 revenues of $6.6 billion, VMware has more than 500,000 customers and 75,000 partners. The company is headquartered in Silicon Valley with offices throughout the world and can be found online at www.vmware.com.

The Best Platform for One Cloud, Any Application, Any Device: Choosing a common platform to manage all your applications, from data center to device, greatly simplifies IT so you can focus less on infrastructure and more on innovation. vSphere is our common platform for virtualized servers and desktops and the VMware vCloud Air secure public cloud. Our vRealize family delivers comprehensive management and automation across your enterprise. AirWatch by VMware provides the enterprise mobility management platform of choice for customers of all sizes. VMware EVO hyper-converged infrastructure systems make deploying software-defined compute, networking and storage fast and simple. Our vast ecosystem of over partners and solution providers and our broad support for the hardware and applications you already own make VMware solutions easy to adopt.

For more information: www.vmware.com/products/workspace-one/

ABOUT PAC

Founded in 1976, Pierre Audoin Consultants (PAC) is part of CXP Group, the leading independent European research and consulting firm for the software, IT services and digital transformation industry.

CXP Group offers its customers comprehensive support services for the evaluation, selection and optimization of their software solutions and for the evaluation and selection of IT services providers, and accompanies them in optimizing their sourcing and investment strategies. As such, CXP Group supports ICT decision makers in their digital transformation journey.

Further, CXP Group assists software and IT services providers in optimizing their strategies and go-to-market approaches with quantitative and qualitative analyses as well as consulting services. Public organizations and institutions equally base the development of their IT policies on our reports.

Capitalizing on 40 years of experience, based in 8 countries (with 17 offices worldwide) and with 140 employees, CXP Group provides its expertise every year to more than 1,500 ICT decision makers and the operational divisions of large enterprises as well as mid-market companies and their providers. CXP Group consists of three branches: Le CXP, BARC (Business Application Research Center) and Pierre Audoin Consultants (PAC).

For more information please visit: www.pac-online.com

PAC's latest news: www.pac-online.com/blog

Follow us on Twitter: @PAC_Consultants

Contact:

Matthieu Page
Account Manager

CXP Group – Digital Business Services BU (PAC UK)

+44 (0)20 7553 3961

m.page@pac-online.com

ABOUT KUPPINGERCOLE

Europe's leading Analysts on the topics of Information Security in the era of Digital Transformation

KuppingerCole, founded in 2004, is an international and independent Analyst organization headquartered in Europe. The company specializes in offering neutral advise, expertise, thought leadership and practical relevance in Information Security, Identity & Access Management (IAM), Governance (IAG), Risk Management & Compliance (GRC) as well as all areas concerning the Digital Transformation. KuppingerCole supports companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges. Maintaining a balance between immediate implementation and long-term viability is at the heart of KuppingerCole's philosophy.

Research

As a core element of KuppingerCole's research the company provides different types of reports with thought leadership and a vendor-neutral view on the status of the markets, products, and vendors. KuppingerCole's qualified analysts continuously research and update the company's online research library, and perform manufacturer-independent advisory services.

Events

Further, KuppingerCole organizes conferences, workshops, and webcasts in all fields of identity focused on information security, IAM, Cloud, Digital Risk and Digital Transformation. KuppingerCole's yearly European Identity & Cloud Conference is Europe's leading event for thought leadership and best practice in this area and covers the latest and future topics regarding the challenges in digital business.

Advisory

KuppingerCole is the best advisory partner in making your business successful in the era of Digital Transformation.

For more information about KuppingerCole and our services please feel free to contact us at any time.

Contact:

Petra Ehweiner
Product Manager
KuppingerCole

+49 (0)211 237077-19

pe@kuppingercole.com

DISCLAIMER, USAGE RIGHTS, INDEPENDENCE AND DATA PROTECTION

The creation and distribution of this study was supported by KPMG, VMware, Computacenter, CyberArk and SailPoint.

For more information, please visit www.pac-online.com.

Disclaimer

The contents of this study were compiled with the greatest possible care. However, no liability for their accuracy can be assumed. Analyses and evaluations reflect the state of our knowledge in April/May 2016 and may change at any time. This applies in particular, but not exclusively, to statements made about the future. Names and designations that appear in this study may be registered trademarks.

Usage rights

Independence and data protection

This study was produced by Pierre Audoin Consultants (PAC) in cooperation with KuppingerCole. The sponsors had no influence over the analysis of the data and the production of the study.

The participants in the study were assured that the information they provided would be treated confidentially. No statement enables conclusions to be drawn about individual companies, and no individual survey data was passed to the sponsors or other third parties. All participants in the study were selected at random. There is no connection between the production of the study and any commercial relationship between the respondents and the sponsors of this study.

A CXP GROUP COMPANY