ovum

Pirean: Providing a single point of control for business and consumer-focused identity management

The ability to manage the complete digital lifecycle is a key business requirement

Summary

Catalyst

Knowing and understanding your users and their requirements is a fundamental business issue. However, in today's digital economy, this represents only the starting point of the identity and access management (IAM) journey. Before the end of the decade, people will be networking with business systems via a host of connected devices. They will need a range of facilities that allow them to perform both the simplest and the most complex tasks securely, to collaborate on projects and, importantly, to communicate interactively on their own terms. Digital identity is the driving force that makes all this possible. Therefore, having the ability to know and understand users and their requirements and to identify business opportunities as they arise will be the hallmark of successful companies.

Ovum view

Most enterprises have some form of IAM technology in place. However, this often involves fragmented deployments that were taken on to address specific business issues and, as product selection decisions were made at different times, may include technology solutions from several suppliers. Many of these deployment decisions have also been made with business-to-business (B2B) and business-to-employee (B2E) requirements in mind and don't come close to delivering the facilities needed to address today's digital identity management challenges.

Existing B2B and B2E identity management systems remain relevant within their own environments. Nevertheless, they were originally designed to address the access control requirements of on-premise systems and networks, and many are already struggling to meet the hybrid demands of mobility and cloud. They were certainly not intended to deal with the lifecycle management demands of business-to-consumer (B2C) relationships, and cannot be expected to extend outwards and scale to meet the growing challenges of the always-online, connected world. Very few come close to having the levels of control and extensibility needed to deal with the digital economy of the next decade.

Consumer and business value issues now dominate identity management thinking as organisations look to build on customer relationships and identify new sales opportunities. However, building and improving those relationships can be difficult because of existing restrictions. Digital consumers are often forced into using multiple identities to interact with business systems and services, practices that to most users are unsatisfactory when attempting to access what should be straightforward facilities.

As both competition for new business opportunities and the need to retain existing customers intensify, organisations will need to deploy IAM solutions that are consistent and easy to use, and which don't put unnecessary barriers in the way. IAM technology that recognises and supports business and private users as individuals is needed; the systems that business organisations put in place have to be able to deal with every type of relationship. All users want open, easy-to-use, identity management facilities that are safe at the point of use. They also need security controls that can be automatically activated each time there is the requirement for extra protection.

The security components of IAM retain primary responsibility for controlling access and protecting business systems; they have an inherent responsibility to keep users, credentials, and transactional information safe while also striving to maintain accessibility.

Key messages

- Digital identity is the foundation on which business systems rely.
- Business and consumer demands are changing the requirements for IAM technology systems.
- IAM offers core technology that businesses cannot afford to ignore.
- The Pirean approach to IAM is comprehensive.
- Businesses cannot afford to ignore data-protection or data-privacy responsibilities.
- Integration with business systems is driving the IAM sector forward.

Management summary

Recommendations for enterprises

Both user and business issues must now dominate identity management thinking when organisations are looking for an IAM provider capable of developing business, consumer and citizen relationships and identifying new sales and relationship opportunities.

Enterprises need IAM technology and service provider partners that can deliver value and control across all operational areas. They should be looking at technology solutions that have the range, capacity and scalability to support the usage and security demands of all user groups and take into account all the channels of access and mobile devices that users are likely to demand from connected businesses.

> “Enterprises need IAM technology and service provider partners that can deliver value and control across all operational areas.”

The supporting infrastructure of the IAM systems being considered should be capable of handling anything from light, ad hoc browsing through to the secure protection requirements of high-worth clients and privileged users, and the secure sharing of information between connected devices and systems. They must be able to handle every type of user relationship. Looking to the future, this should include dealing with far more users and devices, and doing so with the levels of scalability needed to support multiple user identities alongside the billions of digital identities in Internet of Things (IoT) and smart city environments.

When choosing an IAM technology partner that can deal with the requirements of the connected business world, it is vitally important to ensure that they have the capability and capacity to support both workforce and customer/citizen environments.

Business organisations need to earn customer trust when there is a requirement to share personal information. To achieve this they need IAM technology solutions that have the capability to help build and support business-to-business, business-to-employee and business-to-consumer relationships.

Digital identity is the foundation on which business systems rely

IAM offers a mature technology base, but changes are needed

The platform-based identity management sector, which includes all products and services delivered under the IAM banner, is mainly targeted at securing the access rights of business-to-business (B2B) and business-to-employee (B2E) workforce relationships. Extending the same processes out to meet the requirements of business-to-consumer (B2C) relationships has been partially successful, insofar as online B2C retail services are flourishing and the more prescriptive relationships between financial institutions and, for example, online banking customers are being maintained.

> “Using the traditional IAM approach can put too many barriers in the way of doing business.”

These levels of success in the B2C space have often been achieved despite outdated technology solutions that don't meet the complete requirements of the businesses involved or their consumers. Using the traditional IAM approach can put too many barriers in the way of doing business. There remains too much emphasis on the stop-and-block mentality of IAM and not enough on promoting customer relationships and usability.

Even within traditional B2B and B2E environments, existing IAM approaches have proved to be too complex, difficult, and costly to deploy beyond the highly secure areas of business where security and regulatory compliance requirements meet. To carry on in a similar vein makes no sense. Current and future business requirements involve knowing more about all types of workforce and commercial users and the things they are likely to do once access has been granted.

Identity management solutions that work for all types of user are needed. Platform-based products that struggle to deliver a single view of the user within the confines of the enterprise are unlikely to cope with burgeoning demands to support operational systems across all available channels, mobile devices and business environments.

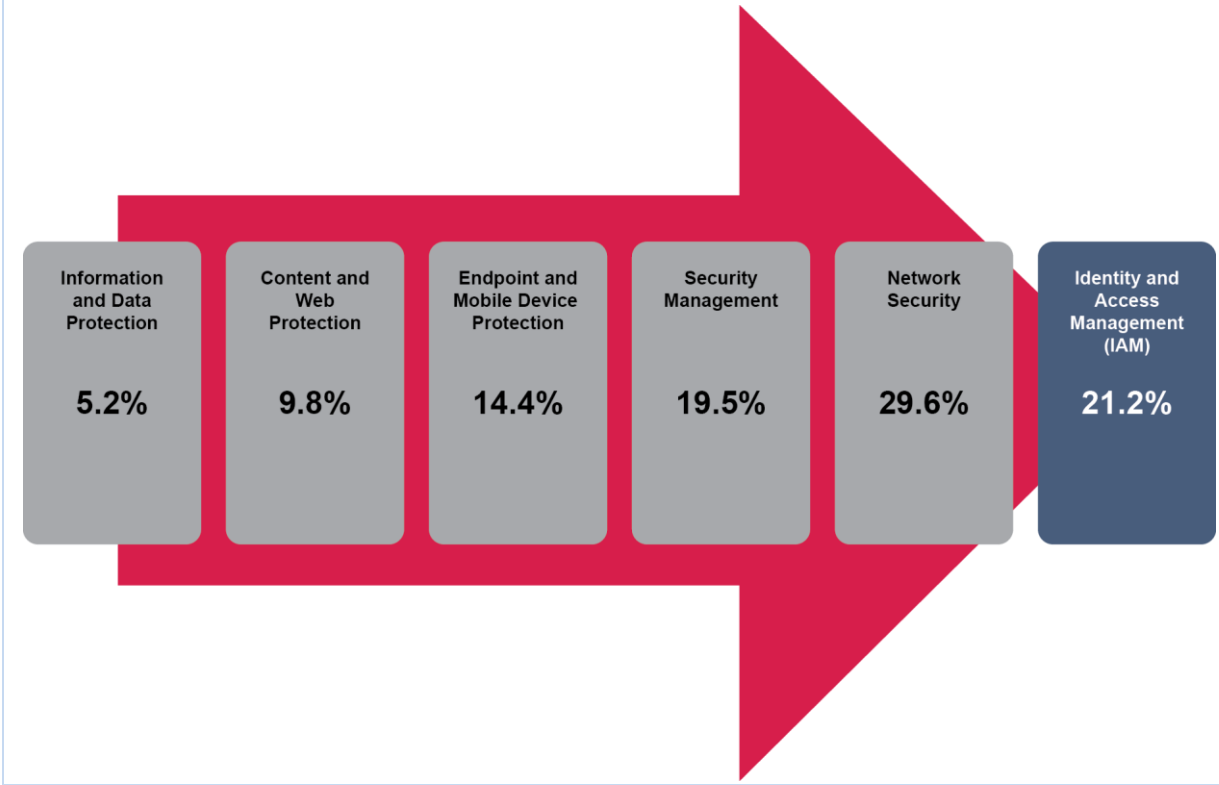
> “Identity management solutions that work for all types of user are needed.”

Industry needs IAM solutions that can genuinely address business and regulatory control requirements across all verticals. It needs technology that has the capacity to support the usage and security demands of all user types when accessing information from all available access channels and mobile devices, and it needs this at a scale that can deal with always-on, connected business operations.

Identity management has to support all the operational and protection requirements of the business and its users

Understanding and having the ability to manage all forms of digital identity is a vital requirement. The need to manage B2B and B2E workforce relationships is not diminishing. IAM accounts for over 20% of enterprise security software spending, as illustrated in Figure 1.

Figure 1: Current enterprise security software spending levels



Source: Ovum

If anything, access controls need to be improved and usability enhanced. Across all trading areas, business-to-user relationships are changing; business users and consumers no longer want the restrictive IAM relationships that previous generations have been forced to accept. All types of users have to be supported, helped to do business, and encouraged to enter into mutually beneficial relationships.

Traditional IAM relationships must change as the requirement to deal with far more users and devices takes over. The levels of scalability needed to support multiple billions of digital identities in Internet of Things (IoT) and smart city environments will push the identity management boundaries, and will also be relevant when determining what the new digital identity model needs to include.

In this context, all users must be recognised as consumers of products and services. The supporting infrastructure has to be able to deal with anything from light, ad hoc browsing through to the secure protection requirements of high-worth clients and privileged users, and the secure sharing of information between connected devices and systems.

> “Traditional IAM relationships must change as the requirement to deal with far more users and devices takes over.”

The delivery of a single view of individual users/consumers is frequently put forward as the key requirement as organisations strive to know more about the individual, their likes and dislikes, and their wants and needs, and to build more meaningful and commercially viable relationships. As such, organisations need to get better at the management and integration of digital identity. They have to extend coverage to manage users/consumers with multiple identities and understand the full extent of these relationships through identity integration.

Consumers of business services who want to gain access to information, products, and services using online channels and mobile devices of their choice need to be supported by the identity management services that each organisation has. More needs to be done on the use of social identity and its role when starting to build business relationships. In this context, more should also be done to reduce identity complexity and to encourage and promote the use of a single common and acceptably secure identity credential across the B2C relationship lifecycle.

> “When choosing an IAM technology partner that can deal with the requirements of the connected business world, it is vitally important that they have the capability to support workforce and customer/citizen environments.”

Many of the things that are relevant to enhancing B2C relationships also apply when looking to improve B2B and B2E workforce interactions and when viewing/monitoring their activities once access has been granted. Having a complete view of every user becomes the key to knowing more about how relationships should be managed and how controls need to be applied to achieve the twin goals of promoting business activity and keeping users and business operations safe.

Building more meaningful and commercially viable relationships can be achieved by working with IAM technology partners, such as Pirean, that are able to deal with the major elements of the B2B, B2E, and B2C digital lifecycle from within a single common identity management solution.

When choosing an IAM technology partner that can deal with the requirements of the connected business world, it is vitally important that they have the capability to support workforce and customer/citizen environments. Coverage has to include all user types and all channels of access when digital identity is used as a passport to online products and services. Businesses cannot afford to ignore any of these issues and must offer support for all appropriate applications and services whether delivered on-premise or from the cloud.

Business and consumer demands are changing the requirements for IAM technology systems

There is an urgent need to improve restrictive processes and make it easier to access information

Users find the existing generation of business-centric IAM solutions outmoded and restrictive. This applies to business users and customers. Of these major groups, business users are more likely to accept the reasons why restrictions need to be in place. The same cannot be said of customers and consumers of business services, who have the option to go elsewhere if working with an organisation becomes too difficult or controls too restrictive.

> “Users – business and social – want access to technology systems from smart devices, unrestricted access channels, and the availability of mobile apps that are constantly being updated as requirements change.”

Fragmented approaches to service delivery and security that are more complex than necessary define many of the silos of B2B and B2E identity management technology currently in use. Whilst at some levels this might still be acceptable for employees, who have become used to the situation, it is far too

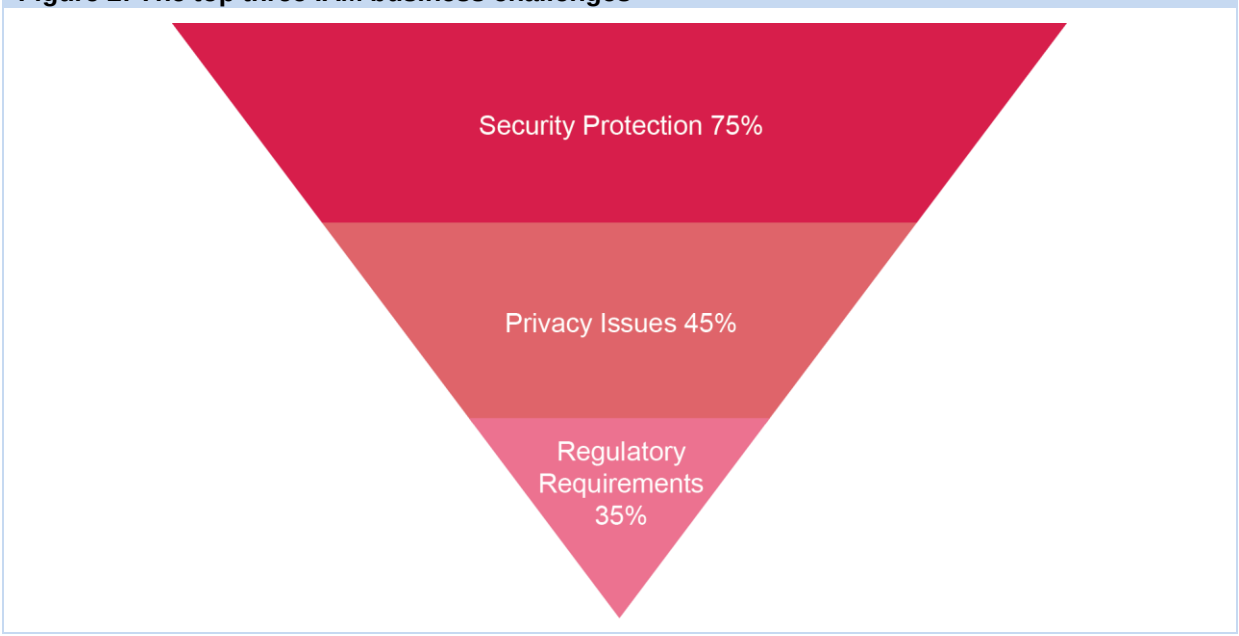
inconvenient for customers to deal with and, significantly, won't be good enough for a new generation of business users who have grown up using consumer technology.

Users – business and social – want access to technology systems from smart devices, unrestricted access channels, and the availability of mobile apps that are constantly being updated as requirements change. What this means to competitive businesses is this: monolithic and restrictive infrastructure systems have no place in the fast moving, opportunistic world of user/customer-responsive identity management.

The need for security and user protection never goes away

Having put the case for IAM systems that offer ease of access and which help businesses to know more about their users, we should be clear that the need for best practice security doesn't go away. Ovum research shows that the top IAM challenges identified by business organisations relate to security, privacy and regulatory issues, as shown in Figure 2.

Figure 2: The top three IAM business challenges



Source: Ovum

There is, in fact, a solid case for stronger security. Because of the global impact of data breaches and credential theft, businesses need to increase their levels of protection, not reduce them. Identity-driven security that is relevant to the modern enterprise and its digital services needs to be always available, be delivered automatically and, wherever possible, not get in the way of doing business. That said, at the right time the visible presence of security encourages customers to commit and complete transactions that would otherwise be abandoned.

When considering the business and user changes needed in an IAM sector that has always focused on restricting access to corporate systems, one of the key factors that can help improve how services are delivered is the ability to maintain relevant levels of control over all elements of identity. For example, this could mean using centrally managed audit and policy control facilities to provide a central source of accessibility and management and include monitoring, alerting and reporting services to highlight unusual activities. This involves combining the best components and practices of core IAM technology with the newer requirements for customer interaction, supporting multi-device

usage and having the ability to identify users as individuals, irrespective of the devices or channels of access they choose to use.

IAM offers core technology that businesses cannot afford to ignore

IAM must evolve to meet next-generation business requirements

IAM functionality that has been developed and honed within the platform environment over the last two decades will continue to be the driving force of future digital identity initiatives. Authentication, access control, user provisioning and single sign-on (SSO) remain the foundations upon which future solutions are being built. However, these core components are already changing along with the supporting infrastructure services needed to deliver IAM services to a larger and more demanding audience.

> “The successful vendors will be those who have already determined which components of IAM can be taken forward and which are no longer relevant and won't scale to meet future demands.”

Issues to be addressed by the established and the upcoming generations of IAM providers involve usability, capacity, scalability and lifecycle management and the ability to offer the all-round coverage needed to deal with the many-to-many digital identity relationships that will evolve during the next few years.

The successful vendors will be those who have already determined which components of IAM can be taken forward and which are no longer relevant and won't scale to meet future demands. The core components of authentication, access control, provisioning, and single sign-on will remain. Nevertheless, the way these services will function and the flexibility and scalability needed to support the next generation of IAM will look significantly different from the restricted and targeted B2B and B2E siloes that most organisations currently operate.

The challenge for vendors, such as Pirean, that provide IAM solutions tailored to meet the specific needs of the enterprise is to build and deliver identity management facilities that fit neatly alongside the operational systems currently deployed by client organisations and at the same time meet their usage and protection requirements.

User authentication will remain a core component

Flexible and intuitive authentication services will be needed to support and control the different relationships between public and private sector organisations, their users and their access requirements. Authentication services must evolve to become more risk-based, adaptive and context-led. This will involve step-down as well as step-up authentication requirements, as organisations need to offer simpler as well as stronger access control protection when situations demand it.

Despite the high-profile security breaches that continue to make headlines, well-managed authentication controls can and should be made simpler and more user friendly. Most users don't need access to sensitive company information. Consumers of products and services should be able to go about their online tasks without interference and without having to remember different passcodes

to gain access to ordinary business services. Most business users also have very ordinary information access requirements and, if they are not trying to access sensitive information, should not be required to pass overcomplicated security checks to do their job.

> “Authentication services must evolve to become more risk-based, adaptive and context-led.”

Machine-to-machine (M2M) and system-to-system (S2S) interactions need to use automated authentication services, and this is where simplicity and security have to come together in order to facilitate continuous access and at the same time ensure that passcode credentials are kept safe and can only be shared securely.

Where appropriate, access and usage controls do need to be stronger. The argument in favour of deploying more effective security controls has been strengthened by the number of security breaches that have been initiated by hackers using stolen credentials, or when insiders have misappropriated company-sensitive information using other people's credentials.

For consumers, stronger security services, which include risk-based, step-up authentication, should be applied when personal information is shared. When purchases are made or when access to personal or financial information is needed, consumers should expect to see visible forms of secure authentication being used.

Business users who request access to more sensitive information sources should undergo additional security checks and the use of risk-based authentication rules should be applied. M2M and S2S interactions should have similar step-up authentication checks and these ought to be performed without interrupting automated workflows.

The key message when addressing the requirements for ease of use and additional security is to get the security and user protection balance right. It is about matching business and user protection with the need for ease of access to build effective business operations and improve business-to-user/consumer relationships.

Single sign-on (SSO) services need to take up the digital identity challenge

SSO is a key component for managing user credentials and for delivering flexibility. For more than a decade SSO has been positioned as the vital link that enables users to move easily between business systems and, once signed in, retain their credentials for automated reuse as they access on-premise, cloud, and web-enabled applications. However, even in more mature platform environments, across-the-enterprise SSO remains something to which organisations aspire, but which they often struggle to achieve.

> “SSO is a key component for managing user credentials and for delivering flexibility.”

In the next-generation, always-connected world of IAM, organisations need to have SSO services that can maintain a single source of control across on-premise, cloud, and web-based applications. Such services need to incorporate federated capabilities to deal with all types of B2B, B2E, and B2C relationships that involve business partners, supply chain services and third-party products and services.

SSO must offer secure seamless access from all available devices, support unencumbered movement between systems and applications and, at the same time, help to improve the customer experience. Federated SSO extends accessibility by enabling movement across organisational

> “ SSO must offer secure seamless access from all available devices. ”

boundaries to partner sites/services. Then, to be more effective, it must support key industry standards such as SAML, OAuth, WS-Fed, WS-Trust, OpenID and OpenID Connect.

Provisioning and de-provisioning remain important elements of control

Provisioning and, importantly, having the ability to close down access using de-provisioning facilities once a user's rights have been revoked are key management components in the IAM portfolio. Irrespective of industry vertical, public and private sector organisations need to be in control of all their users, and the most effective and efficient way to achieve this is with provisioning systems that are up to date and have the ability to adapt to everyday change-management requirements.

Automation and management of provisioning services has to fulfil several important business and user mandates. One of these is the need to centrally manage what individuals and user groups are allowed to access, including the policy and rule-based controls that have to be in place to ensure that each user is who they claim to be, that each device is registered to the user or is acceptable for the task/interaction in hand and that the selected device and channel of access is safe and fit for purpose.

The user-accountability side of the equation will often benefit from self-service ownership where users take ownership and responsibility for updating credentials and for submitting requests for different levels of access for their digital identity. For business organisations, the self-service benefits proposition is an important efficiency driver, and when supported by a full range of user monitoring, alerting, reporting and management services, adds extra security and data protection to the overall user access package.

In the B2C arena, good quality self-service provisioning can be used to help improve user experiences. Easy-to-use and consistent registration and change management services can be delivered using self-service and, where ease of access is genuinely part of the equation, both sides of the consumer and the business relationship benefit.

> “ In the B2C arena, good quality self-service provisioning can be used to help improve user experiences. ”

For business organisations and their customers, provisioning services need to offer a variety of user on-boarding facilities, ranging from individual self-service registration to bulk data uploads. Automation is then required to provision users to the most suitable set of applications/services and link these back to user self-service functionality to deal with password changes or updates to profile information.

In both customer- and business-facing environments this type of functionality can help improve user experiences, providing them with more control over credentials, while also reducing operational overheads.

IAM needs to focus more on the identity lifecycle

Identity-based usage and security has to match the changing requirements in each phase of the business-to-user relationship. As shown in Figure 3, the complete customer lifecycle needs to be

supported, and this applies to relationships between all types of user as business-to-consumer, business-to-employee, business-to-partner, and business-to-supply-chain relationships evolve.

Figure 3: Customer lifecycle requirements for IAM

Source: Ovum

The access, usage, and security issues are likely to be more fluid and transaction-driven where B2C relationships are involved, whereas in B2B and B2E environments more measured and structured relationships are the norm.

> “As relationships progress and users begin to conduct business, that is the time to balance convenience with user safety and data protection.”

When building B2C relationships, the use of social identities can offer a level of authentication that is good enough to begin with. Its use acknowledges that customers should have the opportunity to view the goods and services that an organisation has to offer easily and conveniently and on the customers' own terms. As relationships progress and users begin to conduct business, that is the time to balance convenience with user safety and data protection.

In fact, common themes that reoccur across all user groups involve the need for ease of access and the application of appropriate levels of security controls when the time is right. Across B2B, B2E, and B2C environments, there are three major challenges:

- Simplifying registration and delivering self-service facilities and, where feasible, offering seamless access to applications that are appropriate to consumer interests or business-related activities.
- Protection requirements that need to be appropriate across all phases of the user lifecycle, and appropriate to the sensitivity of data being accessed or information being shared.

- Provisioning and authenticated access to products and services must be convenient and secure and have flexible enough step-up and step-down capabilities to deal with usage requirements that constantly change.

The benefits of monitoring, reporting, audit and security intelligence are needed

Business organisations need to know more about what their users are doing and what their activities indicate about future commercial prospects, while at the same time having a better picture of threats to the business. For business opportunities, organisations need to know more about user interests, the products and services they appreciate and the things they are likely to buy. For security and compliance purposes they need to monitor access and consider normal and unusual usage patterns in order to detect data breaches/data theft and other risky activity.

> “Areas that add to the overall protection proposition include monitoring and recording of log-on and session event activity.”

Areas that add to the overall protection proposition include monitoring and recording of log-on and session event activity. Alerts sent to security administrators should be based on the usage restrictions set: rules and policies that are being applied to session and network usage. Examples could include alerts for predetermined access events – failed log-on attempts, attempts to access default accounts, out-of-hours activity, etc. The monitoring and alerting components should target suspicious network activity, so that the information can be used to help systems administrators prioritise their threat management workloads.

In support of business opportunity engagements, organisations need to monitor and analyse access requests and usage to better understand the things their customers like and are interested in pursuing. This is relevant to the provision of information that helps businesses to respond to user requirements, build relationships and share opportunity information with partnering business systems.

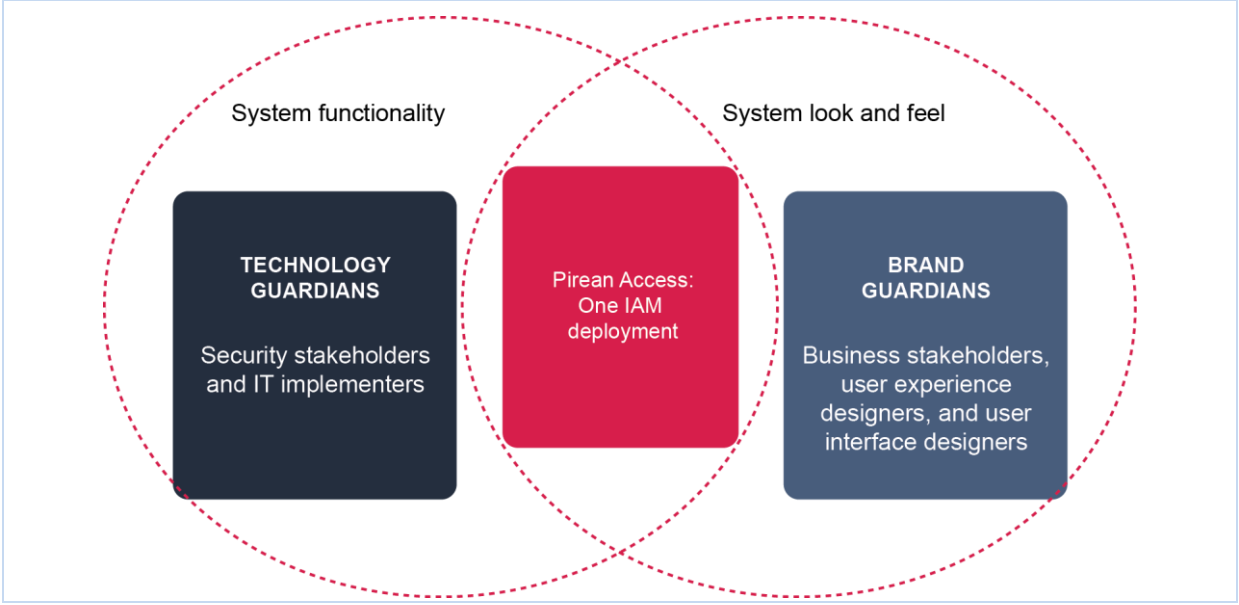
The Pirean approach to IAM is comprehensive

Pirean addresses the identity lifecycle for consumers, the workforce and enterprise

Pirean's Access: One addresses the IAM lifecycle requirements of all major user groups. Its brand-aware approach to IAM helps move enterprise organisations away from the restrictive, stop-and-block silos of identity management that are still prevalent today. It focuses on the delivery of consumer-facing services that reflect the brand image, business values and online character of the client organisation. Pirean's use of technology and supporting professional services combine to address the enterprise demands of IAM users across the spectrum of B2B, B2E, and B2C environments.

As shown in Figure 4, Access: One brings together and surfaces the centralised management controls and workflow processes needed to deal with the different user groups, including technology and brand stakeholders. And because of its brand-aware focus, it addresses the multiple trading images and federated delivery relationships that enterprise organisations need to deploy.

Figure 4: Integrating Pirean Access: One across business and operational environments



Source: Pirean

As organisations search for next-generation IAM solutions that are capable of dealing more effectively with users that want access to products and services on their own terms, it is clear that existing, legacy IAM approaches have to change. By the end of the decade, industry predictions suggest that, worldwide, there will be between 5 and 6 billion online users and over 35 billion connected devices in use. The scalability needed to support enterprise access in customer-facing environments will require IAM solutions such as Pirean that can deal with all types of user and at the same time offer the scale and technology infrastructure to handle high-volume and high-usage environments.

> “Pirean's use of technology and supporting professional services combine to address the enterprise demands of IAM users across the spectrum of B2B, B2E, and B2C environments.”

To be effective, the operational focus has to be on making user access easier. This includes providing a better, more consistent, and more manageable view of user activities, and delivering a single common identity management solution that addresses the extensive range of IAM use cases that organisations are likely to bring to the table. It involves having a clear and actionable picture of the acceptable and unacceptable things users do once access has been granted, along with the ability to use the information gathered to build better relationships and generate business opportunities.

The Pirean Access: One approach to IAM offers a single platform and single point of control across workforce, federated business partner and consumer relationships. It deals with the design and the look-and-feel elements of the finished product and aligns this with the defined user experience and data protection requirements set by each client organisation.

> “The Pirean Access: One approach to IAM offers a single platform and single point of control across workforce, federated business partner and consumer relationships.”

For the workforce (including employees, contractors, supply chain etc.,), for business partners, and for consumers (customers and citizens), Access: One opens up user access to voice, mobile, tablet, laptop and desktop devices and channels.

Its identity and access management framework is driven by administration, policy management and workflow layers that build and deliver a single view of each user, their access rights and their interests:

- Identity management deals with the entitlement, role and privileged user management elements across the user lifecycle for people, devices and organisational requirements.
- Access management and its controls are delivered through the integrated use of authentication, authorisation, SSO and federated identity management services.

For Pirean, the unified view of the individual becomes a key component because of the need to deliver access to on-premise, web, and cloud services applications from a common credential. It highlights the need for secure, policy-based, web and enterprise SSO, along with the extended requirement for federated capabilities when dealing with third-party business partners or external divisions of a distributed business. Along with an effective SSO policy comes the need for appropriate and, where necessary, strong authentication, especially when access to sensitive data is involved or when access requests fall outside normal working patterns.

Building and maximising the value of digital relationships is what organisations are now looking to achieve with their IAM investments. To be safe and stay safe remains the overall objective, but with a balance between ease of access and data protection, while taking into account the privacy rights of the individual.

Pirean Access: One provides a scalable, centrally managed platform that brings together the accessibility, monitoring and security components of IAM across core infrastructure platforms, devices and access channels. As organisations grow their online business, they need to have scalable, business-focused and brand-aligned identity management technology that is always available, can operate on the global stage and can seamlessly link all client access channels.

> “Building and maximising the value of digital relationships is what organisations are now looking to achieve with their IAM investments.”

Using identity as an enabler, the requirements of all types of user, from employees and business partners to customers and citizens, need to be addressed securely and unobtrusively. Pirean offers brand-aware consumer-facing services which match the image of the client, and embeds security controls that are presented as a seamless extension of the client website. Its IAM technology is available for deployment on-premise or in the cloud. Pirean also offers Access: One as a service, using its outsourcing identity-as-a-service (IDaaS) capabilities, with the alternative of managed IAM services for organisations that require a supported and managed on-premise solution rather than the remote IDaaS option.

Business cannot afford to ignore data-protection or data-privacy responsibilities

Data protection and privacy are important business issues

Despite the hype around opening up business systems and providing users with the access they need, when they need it, and from any available device and channel, accessibility comes with the

caveat that business and customer data must be properly protected, privacy issues addressed, and user credentials not left open to compromise.

Personal data and the system-access credentials of valid users are as valuable to cybercriminals as they are to business. Organisations have to ensure that the IAM solutions they choose have the security controls needed to keep users and their data safe and that the privacy of the personal data they agree to share with a business cannot be exposed.

> “Personal data and the system-access credentials of valid users are as valuable to cybercriminals as they are to business.”

Data protection and privacy is a frontline business responsibility. However, systems and data protection is more than just a technology issue. Further improvements can be made to the overall position by extending security coverage into an education and training strategy, targeted at helping users to be more aware of their data protection responsibilities and the need to keep user credentials safe.

As such, the key issue for IAM systems remains the need to control who gets access to sensitive data. Because of the many examples of user credential abuse, there is a requirement to understand more about an organisation's users and what they are doing with their access rights. Organisations need to know what normal usage looks like, have the facilities that monitor usage, and set warning flags and send out alerts when unusual behaviour patterns are detected. User monitoring, analytics and threat intelligence services are all needed within the IAM sphere of operations to deliver additional levels of control and protection.

> “Organisations need to have a well thought out data protection strategy to balance open and free user access with the protection of data and the security of financial transactions.”

Organisations need to have a well thought out data protection strategy to balance open and free user access with the protection of data and the security of financial transactions. It is a trust balance issue in which earning customer trust is essential to the prosperity of the business. IAM solutions such as Pirean Access: One are needed to deal with user requirements for ease of access in consumer and workforce environments and for delivering automated security services that meet user and business expectations.

Integration with business systems is driving the IAM sector forward

Organisations need to deliver more business value from digital identity

Security and privacy remain the top challenges for business organisations. The main reason for this is the need to deliver core products and services safely while protecting users and their data. IAM is one of the foundation technologies organisations need to have in place in order to do this, and while this report has highlighted the security and data protection challenges that currently exist when managing digital identities, it is also important to take into account the business benefits that can be gained from building and maintaining a trusted identity management position.

Business transformation openings include the economic benefits and growth opportunities that arise from knowing more about users who access a business's products and services. A greater understanding of their areas of interest and of the likelihood of their becoming a customer in the near future creates opportunities for targeted marketing to increase sales and for up-sell openings based on existing interests and purchases.

> “ Security and privacy remain the top challenges for business organisations. ”

Companies understand the importance of earning customers' trust when persuading them to share personal information. They need technology solutions that help them do this safely and have the capability to support and build relationships. Information gathering can in itself raise privacy concerns, so it is important to achieve the right balance between usability, privacy and data protection.

More needs to be done to deal with smart identity issues

The current IAM focus is on individuals, their business value and the potential threats they pose to everyday business operations. Increasingly, organisations should also be taking into account the ownership and management of smart digital products and services and their communication requirements.

This includes elements associated with the consumer Internet of Things (IoT), smart city services and industrial IoT, and in particular the information these systems and devices have and will be required to hold and their communication and data protection requirements. By the end of the decade there will be over 35 billion smart devices that deliver automated M2M and S2S communications based on device identity and the rules that control how they communicate.

Identity management will be closely tied into their use. Organisations will need to secure and manage these interactions and should consider the benefits of utilising integrated IAM systems to bring together all components of the digital lifecycle.

Organisations will need solutions such as Pirean Access: One to deliver the right mix of technology, systems expertise and supporting professional services to build scalable identity and access management solutions that are right for the business and for its complete range of users.

Appendix

Author

Andrew Kellett, Principal Analyst, Infrastructure Solutions

andrew.kellett@ovum.com

Copyright notice and disclaimer

CONTACT US

www.ovum.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo