INDUSTRY INSIGHTS: IDENTITY IS THE NEW PERIMETER
### Table of Contents

- **03** Meet the Modern Enterprise
- **07** The Connected Consumer
- **10** What Does Next Gen Identity Look Like?
- **14** Identity and Access Management in Action
- **15** Moving IAM Forward

### Sources
2. CIO, Spotlight on ‘Rogue IT’, A panel discussion on ‘raising the strategic profile of IT’: Part 5 of our special report on the CIO Summit. Stephen Bell and Divina Paredes (CIO New Zealand), August 2013.
3. Computerworld, The Upside of Shadow IT by Julia King, April 2012.
MEET THE MODERN ENTERPRISE
MODERN BUSINESSES ARE MORE OPEN THAN EVER BEFORE, BUT THAT DOESN'T MEAN THEY HAVE TO BE LESS SECURE. LEARN HOW NEXT GEN IDENTITY OFFERS A STRATEGIC FOUNDATION FOR FUELING BUSINESS GROWTH.

Long gone are the days of all on-premises software, where proprietary applications were accessed from within the confines of the corporate firewall over computers issued by the organization, or by consumers from a single web access point. The intersection of mobile, social and cloud offers unprecedented visibility and opportunities for the enterprise, but has also created an environment with multiple (and increasing), disparate user identities across touch points—placing additional barriers between your customers and your organization. As we move toward a completely connected and always-on world, effective identity and access management (IAM) is critical—both for enabling secure business and to meet the demands of today's savvy consumers.

Learn how these trends are impacting your enterprise, the limitations that exist within legacy identity and access management (IAM) solutions to address them, and how the pillars of the Next Gen Identity™ platform will enable you to future-proof your identity strategy to any business scenario, drive business agility and improve end users’ experiences across your ecosystem.
A MOBILE-FIRST WORLD

Mobile is no longer a developing trend. While enterprise may still recognize certain advantages of web applications over native (notably deployment and ease of update, etc.), both enterprise employees and consumers are voting with their fingers in favor of the native model. At least currently, the advantages that native apps typically have in UI, UX, usability, etc., have led them to become more and more popular with users.

Many businesses invest heavily in a security regime that works for web applications, but it doesn’t necessarily extend to mobile apps. Emerging identity standards such as OpenID Connect and OAuth 2.0 offer a consistent experience for user authentication across web and mobile applications. OpenID Connect allows you to always send your users to the same place to authenticate, so that you see what your users are doing under all circumstances and you can apply the full force of your security tools. Users get a consistent experience everywhere. In addition, the same standards can be used to secure identity-based API access to applications.

As mobile usage eclipses desktop usage and users increasingly favor native applications, your identity and access management solutions must treat mobile and API access as equal classes.
IN THE CLOUD

The trend toward IaaS continues to grow—creating a hybrid IT landscape combining multiple cloud and on-premises environments under the management of a single enterprise. As more enterprises evolve their cloud strategies, they are faced with legacy IAM stacks that were never meant to exist outside the enterprise and are realizing that secure access and authorization to infrastructure-as-a-service (IaaS) is a significant impediment to execution.

DO IT WITHOUT IT

In a recent customer survey, we noticed an alarming trend: 60 percent of our customers have completed IT projects that connect to Software as a Service (SaaS) applications without their IT organizations even knowing about it! These activities open your company up to security vulnerabilities; exposing you to regulatory action and diminished brand trust.

A McAfee market research survey found that more than 80 percent of respondents admit to using non-approved SaaS applications in their jobs. The most shocking and ironic part? IT employees use a higher number of non-approved SaaS applications than other company employees!
THE CONNECTED CONSUMER
USHERING IN THE POST-PASSWORD ERA

Perhaps the most alarming “trend” is the continued abuse of IAM’s albatross: the password. Companies are spending more than $40 billion on IT security technology while hackers cost the U.S. economy as much as $100 billion every year, and the undisputed majority of these breaches are password-related. These economics tell a clear story: security approaches that target endpoints, networks and email are not equipped to cope with the increasingly mobile and cloud-connected world in which we live.

THE CONNECTED CONSUMER

Today’s hyper-connected, highly distracted consumers have expectations that are changing the notion of customer experience from every angle. Armed with multiple devices, customers are increasingly demanding flexible and frictionless access to data from anywhere. In recent years we have seen the emergence of a new reality in people and device computing. From thermostats to smartphones, everything is connected to the Internet and, as a result, everything is exposed to a security breach. The Internet of Things (IoT) is changing everything—including the security landscape.

THE INTERNET OF THINGS WAS “BORN” BETWEEN 2008 AND 2009

World Population

- 2003: 6.3 Billion
- 2010: 6.8 Billion
- 2015: 7.2 Billion
- 2020: 7.6 Billion

Connected Devices

- 2003: 500 Million
- 2010: 12.5 Billion
- 2015: 25 Billion
- 2020: 50 Billion

Connected Devices Per Person

- 2003: 0.08
- 2010: 1.84
- 2015: 3.47
- 2020: 6.58

More Connected Devices Than People

E-BOOK

IDENTITY IS THE NEW PERIMETER
BIG IDEA: IDENTITY AS THE NEW PERIMETER

Today’s enterprise must validate users based on identity along with specific attributes such as role, privileges, location and device, regardless of where the request originates and where the data resides. Unfortunately, traditional security systems weren’t built to extend security beyond the rewall and rely on an increasingly outdated (and vulnerability-riddled) paradigm of usernames and passwords.

As a result, traditional security perimeters must give way to a virtualized world where trusted and federated identities can shape a new security perimeter: identity.
WHAT DOES NEXT GEN IDENTITY LOOK LIKE?
The next generation of identity platform solutions solve for the security and control needed in today’s cloud-connected, mobile-first, post-password world by:

- **Addressing all identity types** (employees, customers and partners) across all channels (web, mobile and APIs)

- **Encompassing every company resource** (internal, private or public cloud), from any device (desktop, tablet or mobile), in any location (inside or outside the network)

- **Embracing open standards**

- **Offering flexible deployment options** (100 percent cloud, 100 percent data center or hybrid environments) to replace or extend legacy stacks for enterprises shifting emphasis towards cloud and mobile platforms, while delivering mission-critical security that cloud-only cannot provide.

- **Building a federated-by-default environment** connecting enterprises across multiple domains inside the firewall and out.

- **Acting as a cornerstone** in the evolution away from passwords and into strong authentication factors.
WHAT DOES NEXT GEN IDENTITY LOOK LIKE?

NEXT GEN IDENTITY PLATFORM

Next Gen Identity extends the federated architecture to the enterprise—managing identity as the perimeter. With open standards at the core, the complexity of administrating all of the identity and access connections is reduced while the reliability and extensibility is increased.

The Ping Identity® Next Gen Identity platform facilitates trusted interaction among groups of application providers and consumers on the Internet, through APIs and from any mobile or desktop screen.

LEGACY SECURITY MODEL

- Proprietary
- On-premises
- Web-only
- Single Domain

NEXT GEN IDENTITY MODEL

- Open standards
- Hybrid, datacenter and cloud
- Web, APIs and mobile
- Federated by default

IDENTITY IS THE NEW PERIMETER
FEDERATED ARCHITECTURE Ping Identity connects any user to any application from any device using any identity authority. Companies have long ago abandoned the aspiration of a single identity system of record for all end points, whether customer, partner or employee utilized. Federation is necessary to connect disparate identity stores.

WEB, MOBILE AND API SECURITY Ping Identity delivers an off-the-shelf solution to secure applications and APIs for partners and developers. Companies can now create a path from their legacy web access management (WAM) solutions to their next generation mobile and API needs.

UNIFIED MANAGEMENT Ping Identity reduces the complexity and risk associated with managing public and private cloud environments through a uni ed approach to security infrastructure and service administration.

CLOUD-CENTRIC As enterprises increasingly move to the cloud, the need for private and public cloud interoperability is a business requirement. Ping Identity is a recognized leader in identity-as-a-service (IDaaS), regardless of the deployment mode, and is the only vendor today that is recognized for leadership across the complete spectrum of traditional IAM and IDaaS.

SELF SERVICE Ping Identity offers a user-driven on-boarding experience for customers and partners, eliminating the need to engage administrators. IT organizations benefit from a self-service model as they add new applications and integrate with legacy and cloud environments.

OPEN STANDARDS Ping Identity materially invests in the advancement of identity standards via our participation in the standards bodies. This work provides industry-wide bene ts and enables us to create useful features and deliver broad interoperability in advance of our competitors.
IDENTITY AND ACCESS MANAGEMENT IN ACTION
IDENTITY AND ACCESS MANAGEMENT IN ACTION

CISCO CUSTOMER SUCCESS STORY

CUSTOMER VITALS: The worldwide leader in networking that transforms how people connect, communicate and collaborate

CHALLENGE: Like many enterprises, Cisco’s growth over the years has left them with disparate authentication tools and multiple legacy IAM stacks across multiple business units. The result was a costly and complex identity and access management environment that hindered their ability to offer single sign-on to their supply chain, demand chain and internal users, creating poor user experiences with multiple sign-ons across applications.

SOLUTION:

- SSO and federated identity
- User provisioning and deprovisioning
- User management
- Application integration

STRATEGY: Cisco and Ping Identity worked to create a solution that would deploy in multiple phases. The first phase focused on delivering a holistic identity framework by integrating their various legacy identity managementsystems (CASiteMinder®,Oracle®AccessManager, IBM® Business Units). The second phase was focused on extending their reach to integrate their supply chain and demand chain and begin SaaS integrations for their employees out to SaaS applications.

RESULTS: Using PingFederate and PingOne, Cisco was able to bridge existing business units together under a holistic identity management framework. This simplified framework allowed them to integrate their supply chain and demand chain partners with a federated identity architecture, and deliver a better authentication experience across their user base. Cisco’s Ping Identity solution now supports three million daily users comprised of customers, partners and employees across hundreds of applications.
MOVING IAM FORWARD
One of the toughest challenges facing business and IT leaders today is the delicate balance required to maintain a strong security posture while providing unfettered access to the applications users need most. The reality of the cloud, SaaS, mobile and API economy will continue to add to the complexity of a changing enterprise environment. The IAM solutions perfected for the last century’s web-only world no longer cut it. Your enterprise needs new strategies to ensure that identities are protected and that data and apps can be accessed by any trusted user, anywhere, from any device.

Today’s most forward-thinking companies are adopting a new, next generation architecture with identity serving as the security perimeter of the enterprise. Based on federated technologies, this approach extends existing identity and access management systems and SSO to the cloud—eliminating passwords and strengthening authentication.

Are you curious about how identity as the security perimeter can move your business forward? Check out Beyond the Firewall, 17 Questions to Ask Your IAM Vendor and Forrester Research’s® Analyst Report: Total Economic Impact of the Ping Identity Identity and Access Management (IAM) Platform for more information.

Or, for even more details on bringing your identity and access management solutions into the new century, please contact Ping Identity today at U.S. toll-free 877.898.2905 or +1.303.468.2882, email sales@pingidentity.com or visit pingidentity.com.