IDENTITY SECURITY TRENDS IN THE MOBILE ERA
<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>04</td>
<td>INTRODUCTION</td>
</tr>
<tr>
<td>06</td>
<td>INSIGHT #1: PRODUCTIVITY AND USER EXPERIENCE TRUMP EVERYTHING ELSE</td>
</tr>
<tr>
<td>08</td>
<td>INSIGHT #2: SECURITY IS BOTH A LEADING DRIVER AND A CHALLENGE FOR MOBILE INITIATIVES</td>
</tr>
<tr>
<td>11</td>
<td>INSIGHT #3: EXECs SEE MOBILE DEVICES AS KEY TO THE POST-PASSWORD ERA</td>
</tr>
<tr>
<td>13</td>
<td>INSIGHT #4: ENTERPRISES ARE SEEKING A SINGLE IDENTITY AND ACCESS MANAGEMENT (IAM) SYSTEM FOR WEB, API AND MOBILE ACCESS</td>
</tr>
<tr>
<td>15</td>
<td>LET’S REVIEW: INSIGHTS POINT TO FEDERATED IDENTITY AND ACCESS MANAGEMENT</td>
</tr>
<tr>
<td>17</td>
<td>APPENDIX: PARTICIPANT PROFILE</td>
</tr>
</tbody>
</table>
INTRODUCTION
INTRODUCTION

The business landscape has changed dramatically within just the past five years. Mobile devices, which are effectively powerful personal computers, are everywhere and possess enormous business potential. Gartner® states that, "By year-end 2020, 80% of user access will be shaped by new mobile and non-PC architectures that service all identity types regardless of origin." Additionally, IDC estimates that 55 percent of all smartphones used in business will be employee-owned in 2015. These and other statistics have most enterprises struggling with a host of issues surrounding the use and security of mobile devices for work.

To better understand the mindset and priorities of those who make security decisions for mobile devices in the workplace, Ping Identity conducted a mobility survey in partnership with Gatepoint Research. The results shed light on four main insights into the top challenges and motivations for enterprise mobile initiatives.
INSIGHT #1: PRODUCTIVITY AND USER EXPERIENCE Trump Everything Else
Eighty-nine percent of respondents cite improved user experience as the top development goal for mobile applications. They know that user experience is king. Whether rolling out mobile apps to your workforce or your customers, users expect a great experience and an app that adds value quickly. Deliver less, and your brand will suffer. Eighty-eight percent say the top development goal for mobile applications is improved user productivity. Leading enterprises have discovered that a mobile workforce is a more productive and satisfied one.

“We want to continue to provide our customers with exceptional customer experiences and that means engaging with them where they are—conveniently over their smartphones, tablets or the Internet.”

Eric Barnes, Application Development Manager, Wawa Inc.

Learn more about how WaWa is Staying a Step Ahead of On-the-Go Customers »
INSIGHT #2: SECURITY IS BOTH A LEADING DRIVER AND A CHALLENGE FOR MOBILE INITIATIVES
When respondents were asked about their goals for mobile applications, “Secure, auditable, and compliant access to data” was cited 83 percent of the time.

This was the third most common goal stated, just behind productivity and user experience.
When participants were asked about the issues that constrain their rollout of mobile applications, 71 percent said that, “Security issues over devices caching passwords locally” was a significant concern. Next on the list of issues was, “Inability to scale mobile app development without higher security risks.”

As the participants know, mobile devices pose a unique set of threats to enterprise security. Because the nature of mobile devices, bidirectional access to data occurs beyond the protection of the firewall. And in most cases, passwords are stored directly on the device—exposing the enterprise to risk when a device is stolen or lost. They want to scale their mobile application development to meet the needs of the app economy, but they need to ensure that security scales with their mobile app development needs.

Read about how Land O’ Lakes rolled out simple secure access to mobile apps »
INSIGHT #3: EXECS SEE MOBILE DEVICES AS KEY TO THE POST-PASSWORD ERA
Almost 40 percent of the participants see mobile platforms as a way to provide strong or multi-factor authentication (MFA) as a means to improving security. In addition, they’re seeking simpler, more innovative and lower-cost ways to handle MFA through the use of mobile device applications.

The goal of using mobile devices for MFA is proof that enterprise reliance on passwords as a primary authentication method is starting to break down. They’re moving toward the post-password era—and for good reasons. Among other problems with passwords, the main cause of security breaches and hacks is stolen credentials.

Learn more about transforming smartphones into mobile authentication devices »
INSIGHT #4:
ENTERPRISES ARE SEEKING A SINGLE IDENTITY AND ACCESS MANAGEMENT (IAM) SYSTEM FOR WEB, API AND MOBILE ACCESS
Support for web, API and mobile access was the most common goal cited for future mobile access. This all-of-the-above approach clearly provides the most flexibility to meet current and future employee and customer needs for productivity and user experience. But what about security? Respondents answered that in the following question, where they indicated that a single system that supported web, API and mobile authentication and authorization was the most desirable attribute of an IAM solution.

Read about a modern architecture for identity management »
LET'S REVIEW
LET’S REVIEW: INSIGHTS POINT TO FEDERATED IAM

INSIGHT #1
Productivity and user experience trump everything else

INSIGHT #2
Security is both a leading driver and challenge for mobile initiatives

INSIGHT #3
Execs see mobile devices as a possible solution to insecure passwords

INSIGHT #4
Enterprises are seeking a single identity and access management (IAM) system for web, API and mobile access

These insights underscore the value of a federated IAM system, which is the core of Ping Identity’s solution. Such a solution simplifies and secures the ugly, complex, heterogeneous world of enterprise IT.

The Ping Identity Platform addresses all four insights and more:
- **SSO**—boosts productivity and improves user experience
- **Mobile SSO and API security**—provides a scalable framework to make mobile devices and apps secure and productive
- **Mobile MFA**—transforms a mobile device into a second-factor authentication method
- **Based on standards**—engineered to secure web, mobile, and API security with open standards

Go to pingidentity.com to learn more about how you can address the business insights and trends of this decade and the next.
APPENDIX: PARTICIPANT PROFILE
APPENDIX: PARTICIPANT PROFILE

Participants of the survey represent a wide range of industries, decision-making roles and budgets. One hundred percent of responders participated voluntarily; none were engaged using telemarketing.

Industry Sector: Survey participants represent firms from a wide range of industries. Forty-five percent are in the Fortune 1000.

Revenue: Participants represent firms with a well-stratified range of revenues.

Use of WAM for Mobile App Initiatives: Fifty percent of participants admit that they don’t currently leverage a web access management (WAM) infrastructure to support mobile app development.

Job Level: Survey participants represent senior management and executives in decision-making roles.