FORRESTER®

For: Security & Risk Professionals

Security Risks Faced By Healthcare Providers Empowering Mobile Moments To Clinical Teams

by Chris Sherman and Skip Snow, December 8, 2014

KEY TAKEAWAYS

Healthcare BT Leaders Are Slow To Adopt Mobile Policies, Despite Workforce Demand

Healthcare professionals demand mobile access to the same electronic resources and tools used on their stationary endpoints, ultimately giving them the ability to make faster and more collaborative decisions and increase engagement between hospital employees, systems, and patients.

Security Pros Must Protect Mobile Patient Data From Evolving Threats

In today's black market, the value of healthcare records far surpasses that of credit card information, fetching anywhere from $20 for a single health record to over $500 for a complete dossier. In a mobile world, S&R pros not only have to protect patients' privacy, but protect them from fraud and identity theft.

S&R Pros Must Design Policies That Support Staffs' Mobile Moments

In order to provision mobile access in a secure manner, healthcare security pros must understand how various roles within the provider staff use and access data. Creating a mobile policy set based on each of the "mobile moments" experienced by their respective employee roles should be the end goal of any mobile security strategy.

Security Risks Faced By Healthcare Providers Empowering Mobile Moments To Clinical Teams

by Chris Sherman and Skip Snow
with Stephanie Balaouras, Tyler Shields, and Jennie Duong

WHY READ THIS REPORT

Security pros in the healthcare industry must balance the need for compliance with the Health Insurance Portability and Accountability Act (HIPAA), as well as other security and privacy regulations, with medical professionals' need to have access to patient information anywhere, anytime. Medical professions demand this access in order to speed up decision-making, facilitate collaboration, increase efficiency, and improve healthcare outcomes. This report will not only look at the drivers for remote system access but will show how some of the most mature hospitals and other healthcare providers have done it without compromising privacy and security.

Table Of Contents

Notes & Resources

Forrester interviewed several vendors and user companies, and experts from the healthcare industry.

Related Research Documents

Brief: Stolen And Lost Devices Are Putting Personal Healthcare Information At Risk
September 4, 2014

Industry Spotlight: US Healthcare Security Budgets, Priorities, And Challenges
February 19, 2014

TechRadar™: Enterprise Mobile Security, Q4 2013
December 13, 2013

HEALTHCARE BT LEADERS HAVE BEEN SLOW TO CATCH UP WITH MOBILE TRENDS

Mobile devices, such as smartphones and tablets, and a multitude of apps have irrevocably changed the way healthcare providers operate. Clinicians, healthcare admins, and other support staff work and interact with the business and their customers (patients) instantly and effortlessly through a myriad of mobile apps and device types, giving providers new opportunities to increase productivity and efficiency.

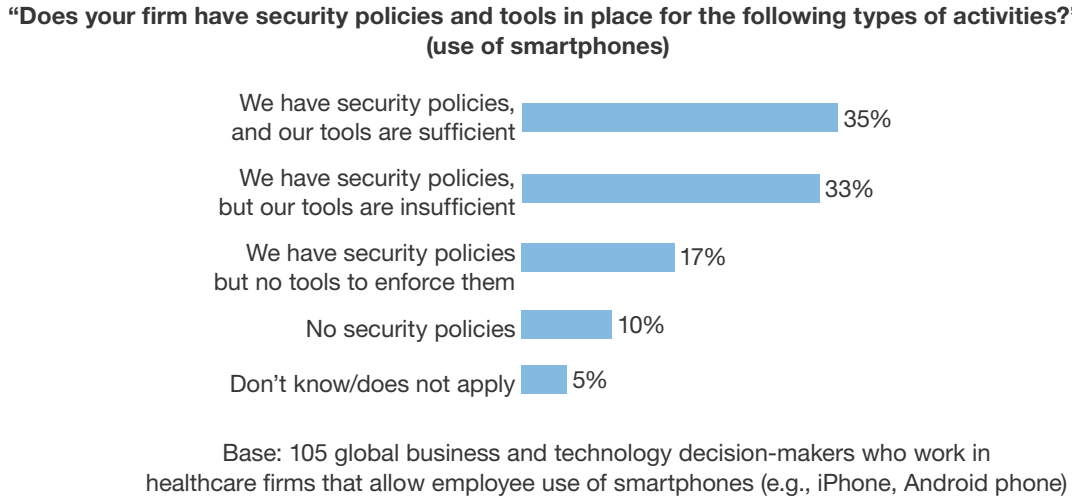
However, while a majority of healthcare providers report widespread use of mobile devices within their organizations, business technology (BT) leaders, especially S&R leaders, have been slow to adopt formal policies to support and secure mobile within their organizations (see Figure 1).[1] We attribute this gap to a number of factors, most notably the:

- **Complexity involved in supporting a variety of device types and software versions.** As vendors introduce new devices, apps, and operating systems (OSes) into the market, attempting to create one-size-fits-all mobile hardware and software policies becomes increasingly futile. Mobile capabilities evolve, and subsequently so do their support requirements. Not surprisingly, BT staff encounter many challenges when trying to build mobile policies that center on specific use cases for specific device types and OS versions. As one director of IT operations within a large US-based hospital system recently told Forrester, "Trying to support all the new devices and apps being introduced into our environment feels like trying to hold onto an 80,000-mph train without falling off."

- **Lack of mobile integration with core care applications.** Many of the clinical data systems, especially the ones used in the acute care facilities of hospitals such as electronic medical records and medical device monitoring applications, were released before mobile devices gained prominence within healthcare. Subsequently, many of these core care applications were developed with traditional computing models in mind, with little to no native support for mobile device access. This leaves it up to BT staff to find ways to serve up these applications on mobile devices using alternate methods, such as app or desktop virtualization techniques.

- **Clinical safety concerns related to mobile access.** Healthcare providers worry that allowing clinicians to manipulate patient records and initiate orders from their mobile devices could lead to increased errors when these actions are taken outside of the clinical environment. Do you really want your physician to make judgment calls from his or her mobile device while having dinner with friends? Add to that a couple of glasses of wine, and one can see how this can become a dangerous (and potentially litigious) proposition if the proper technical boundaries are not in place. Traditionally, when physicians have been consulted by phone, there are supervisory means to ensure that their orders make sense, because they are consulting, not giving orders. Once they actually give orders from a social setting, these checks and balances that have been implicit disappear.

Figure 1 Hospitals Lack The Proper Tools To Protect Mobile Devices



Source: Forrester's Business Technographics® Global Security Survey, 2014

S&R Pros Face Additional Challenges When Securing Clinical Mobile Data

Within BT, healthcare security pros are the ones losing the most sleep at night worrying about the risks posed by mobile device access within their organizations. In fact, Forrester survey data shows that employee-provisioned devices are perceived as one of the top risks overall by healthcare security professionals (see Figure 2). This is not surprising, considering that healthcare security pros must deal with:

- **An evolving set of mobile threats.** Historically, most healthcare BT and security pros have focused on the prevention of privacy abuses rather than other security threats, such as those from cybercriminals who monetize stolen PII and PHI through black markets. One CIO for a large multihospital organization told Forrester: "We are not worried about hackers stealing PHI; they are more focused on credit card and intellectual property, neither of which we carry much of." While this may have been true in the past, now the value of healthcare records far surpasses that of credit card information sold on the black market, fetching anywhere from $20 for a single health record to over $500 for a complete dossier on a patient with driver's license, health insurance information, and other sensitive information.[2]

- **Acute care organizations providing competing solutions to the same physicians.** In most acute care settings (i.e., hospitals), physicians have admitting privileges to a number of hospitals in a region, and these hospital systems often compete for patients within particular markets. So while one institution might want to put one security framework solution onto the phones of one of these physicians, another might want to use another tool set. One can quickly see how

this will lead to problems on these physicians' devices: The solutions might not be compatible, or running many solutions in parallel might prove too much burden for the phone. Thus, the security policies for devices not owned by the institution, especially for those who are not full-time employees of the institution, must have a sufficiently light binary footprint to coexist with other security policies from other institutions where the professional might practice.

- **Data breaches caused by mobile device theft/loss.** As healthcare workers spend more time working outside of the office and the clinic, and work using mobile devices, data loss risk escalates. Compared with all other industries, healthcare sees a greater percentage of security incidents as a result of stolen or lost devices and a greater number of compromised patient records with PII and PHI.[3]

- **Pressure to do more with less.** A lack of funding for security projects (and BT initiatives in general) continue to plague many healthcare organizations, as evidenced by Forrester's survey data as well as anecdotally through Forrester's conversations with healthcare provider security decision-makers. US healthcare organizations are under intense pressure from both payers and government entities to reduce costs without sacrificing healthcare outcomes. This is incredibly difficult; government agencies and payers are reducing payments, yet healthcare organizations' own costs, for pharmaceuticals, equipment, and personnel, are increasing. This puts enormous pressure on BT groups and, in particular, security groups struggling to mature their mobile practice.

- **Increasing HIPAA fines and audits.** Increased audit activity from the US Department of Health and Human Services, Office for Civil Rights (OCR), which enforces the HIPAA Privacy Rule, HIPAA Security Rule, and HIPAA Breach Notification Rule, has caused a stir.[4] Typically, the OCR investigates and resolves thousands of complaints regarding HIPAA violations, many of which result in significant reputational damage and substantial fines. However, the OCR is no longer waiting for complaints; it is actively auditing organizations against its own 77-point protocol. During 2013, the OCR completed audits for an additional 95 organizations. In May 2104, the OCR issued its largest fine to date, $4.8 million to NewYork-Presbyterian Hospital ($3.3 million) and Columbia University ($1.5 million).[5]

- **Balancing the demands for increased quality of care and mobile security.** Clinicians and provider support staff continue to demand increased access to sensitive patient data on their mobile devices, with 28% of healthcare technology decision-makers believing this level of mobile access helps improve overall patient safety, according to a 2014 Healthcare Information and Management Systems Society (HIMSS) study.[6] This can be at least partially explained by the fact that mobile apps are used to accelerate clinical decision-making. For instance, medical staff view medical images using a variety of vendor-supplied apps linking to both cloud-based and traditionally hosted medical image repositories; AirStrip One lets providers access patient data directly from their smartphone, and Modernize Medicine's cloud-based EMR uses the tablet as the default interface. Security professionals often lack the tools and policies to get ahead of these data access trends.

Figure 2 US Healthcare Security Risks For Which S&R Pros Are "Very Concerned"

Top five risks

18%	Employee-provisioned devices (laptops, smartphones, and tablets for business use)
18%	Consumer-oriented communication and file-sharing tools run on resources
17%	Employee-provisioned applications (including software and web services like Facebook and Twitter)
14%	Cost pressures on IT
14%	Virtualization in the data center (e.g., storage, server)

Base: 60 healthcare security decision-makers in the US

Source: Forrester's Forrsight's Security Survey, Q2 2013

MOBILE ACCESS WITHIN HEALTHCARE PROVIDERS SPANS A RANGE OF LEVELS

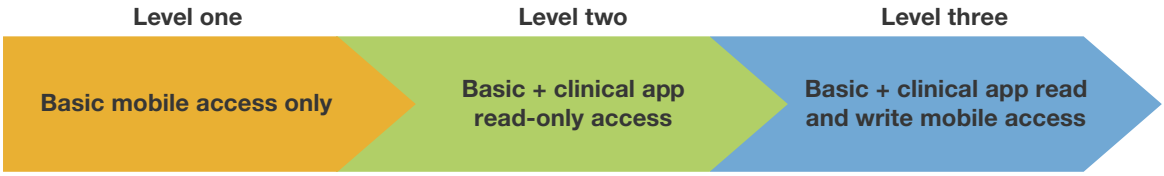
During the past several months, Forrester interviewed a number of healthcare providers, clinical software vendors, and IT consultancies regarding the various levels of data access typically given to both employee-owned and corporate-issued mobile devices within clinical care environments settings. Broadly speaking, the depth and breadth of mobile use within providers can be broken down into three levels of access (see Figure 3):

- **Level one: nonintegrated access.** In this model, BT allows the phone on-premises and allows it to connect to an employee wireless network, or a guest network as a nonoptimal solution, and the medical professional can use the phone for personal or professional reasons, without gaining access to any system that is not available on the public Internet. As the CIO increasingly outsources functions from his BT portfolio, controlling access to corporate functions becomes more difficult, while building a single sign-on infrastructure becomes increasingly important if an institution does want to restrict access to cloud-based software services.

- **Level two: clinically integrated information network with read access.** In this model, core systems such as the electronic medical record are available on the mobile device, but in a read-only mode. This manner of mobile integration, though conservative, is seen as a good way to expose the workforce to the chart, and it starts to inculcate the clinical workflows that incorporate a mobile presence. Epic Systems, for example, partners with Canto and Hiku Labs, granting neither read but not write access to the chart. Epic also offers an HTML5 view of the interface, and many form factors can use this interface, although as specified above, the result does not provide the best employee experience.

- **Level three: fully integrated mobile access.** We see this model significantly less often than the level two model and significantly more often in an ambulatory setting than in an acute care setting. In this model, an employee can use the mobile device to do, for the most part, what he or she can do with a traditional work station. Some electronic medical records (EMRs), such as Modernizing Medicine, were built with the tablet form factor as a core requirement, and we find that many of the cloud-based ambulatory solutions are ahead of some of the major hospital-centric solutions when it comes to mobile abilities. To arrive at a fully integrated model, the security team must think through the risks, and mitigations to those risks, but the care (and overall BT) teams must also think about what quality controls are in place to ensure that medicine is practiced in the most rigorous ways, no matter where the clinician is when he or she writes an order.

Figure 3 The Three Levels Of Mobile Access Maturity Within Providers



113161 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

S&R PROS MUST DESIGN POLICIES THAT SUPPORT STAFFS' MOBILE MOMENTS

To provision mobile access in a secure manner, healthcare security pros must first and foremost understand how various roles within the provider staff use and access data. Creating a mobile policy based on each of the "mobile moments" experienced by their respective employee roles should be the end goal of any mobile security strategy. Examples of this include the moment clerical staff admits a new patient, clinicians require access to critical lab data while bedside with a patient, or custodial staff get called for environmental clean-up services, and countless other mobile moments when access to mobile hospital resources can benefit the coordination of care.[7] For example, a formal mobile policy must answer questions such as:

- **Which employees are allowed mobile access, and to what?** This will vary, based on the information systems access required by specific roles within the organization. For instance, there may be little need to provision mobile access for certain administrative systems, such as patient registration systems eClinicalWorks Practice Management and athenahealth, where the staff never leave their workstations, while physicians and nurses may want to regularly read and write to core care applications such as EMRs Epic and Practice Fusion.

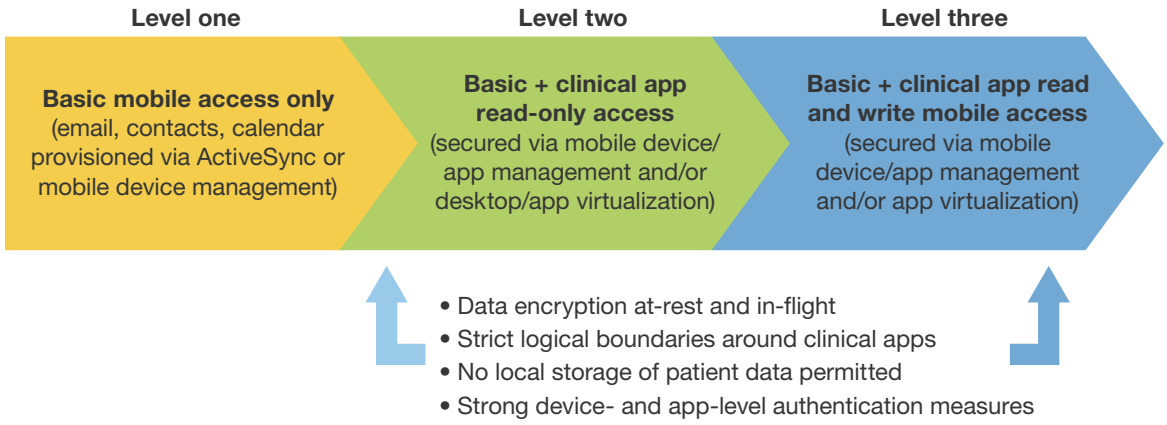
- **Which mobile device types/brands are allowed?** Considering the wide range of device types and mobile operating systems on the market, each with varying native security and management capabilities/requirements, a mobile policy cannot be one-size-fits-all. Your mobile security

policy must dictate which devices are allowed, along with the minimum operating system (OS) version and baseline security posture. For example, one CISO of a network of rural health clinics told Forrester they only allow versions of Apple iOS and Android that offer native device-level encryption so that locally stored patient data remains protected once the device is locked.

- **Are employee personal devices permissible?** BYOD policies will likely vary based on the clinical systems used by the organization as well as the level of mobile access allowed. Considering employees generally protest against strict device-level control over their devices, simple level one mobile access is the common level of access granted to personal devices within many healthcare providers (see Figure 4). A Microsoft ActiveSync profile may be all that users will allow BT to manage on their device in the case of gaining access to corporate contacts, calendar, and email, with the understanding that BT can wipe their device at any time. If users wish to have level two or level three access, a policy of strict logical isolation between the personal and corporate app environment must also be required, with multifactor authentication used wherever an app has write privileges to a clinical core care application.[8]

- **Which data protection policies are necessary to protect mobile patient data?** Your mobile policy must dictate that all patient data remains encrypted when not in use by an authorized individual, whether in transit or stored locally on the device. This includes any messaging system at the employee's disposal, such as email and SMS clients, as well as all clinical or clerical apps with access to patient data. Location-based policies may also be enforced to help reduce the risk of data loss, such as leveraging encryption-based "geofencing" to automatically limit access to certain device functions/apps depending on the employee's location. An example of this would be in the case where stationary administrative staff lose access to patient registration systems on their devices after they leave work. Wherever access to core-care applications are concerned, leveraging a native device or app-specific virtual private network (VPN) is also a best practice due to the highly sensitive nature of these data transactions.

Figure 4 Proper Security Controls Must Be Applied Depending On Mobile Access Level



113161 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

COMPLEMENT YOUR MOBILE SECURITY POLICIES WITH THE RIGHT TECHNOLOGIES

After defining a clear mobile security policy, security pros must work with their counterparts on the infrastructure team (and other business unit leads) to determine which technologies are required given their specific levels of mobile access and security policy requirements.[9] Some of the most common technologies used to protect mobile devices within the healthcare provider space include:[10]

- **Mobile device management (MDM).** Whenever patient data can find its way onto a mobile device's permanent storage, device-level protection is necessary regardless of the level of access. Microsoft ActiveSync or mobile device management solutions, such as those offered by BoxTone, Kaspersky Lab, McAfee, and Sybase, are typically used in these situations. In fact, six out of the nine healthcare providers Forrester interviewed for this report used either ActiveSync or MDM within their environment, typically with MDM used on corporate-owned devices and ActiveSync on their personally owned counterparts (due to its relatively light impact on the device's native user experience). These technologies can enforce device-level protection measures such as pin entry and native OS encryption, as well as a variety of strong authentication measures.

- **Mobile application management/containerization (MAM).** Often used to place a logical barrier between healthcare apps with access to patient data and the rest of the device, MAM software focuses on controlling the specific apps used by employees rather than the device. Unless patient data is allowed to be saved outside of these applications, MAM solutions give S&R pros the ability to worry less about the device environment and focus more on protecting apps and any patient data accessed through those apps. There are a variety of technologies on the market that accomplish this, including "app-wrapping" solutions such as Citrix, MobileIron, and Mocana. Another permutation of app-level management includes app containerization, specifically those solutions that execute clinical/clerical apps within a "sandbox" designed for a high level of isolation between the apps and the rest of the device. Example vendors offering containerization technologies include Citrix, Enterproid, Good Technology, and Tangoe.[11]

- **Mobile, desktop, and app virtualization techniques.** Virtualization techniques can help serve up highly sensitive core-care applications to a mobile device with little to no storage of any patient data on the device. Generally this type of technology is reserved for level two and especially level three mobile access; however, this sometimes comes at a price. If the clinical application delivered is designed for a desktop or laptop (using a mobile client such as Citrix Receiver), it can lead to user frustration when software controls are not intuitive or easily accessible from the smaller touch-based mobile form factor. In fact, numerous clinicians have told Forrester that when core-care desktop applications are delivered to their mobile in such a way, it is often challenging to use in a fast-paced environment. Until more native mobile applications are released by core-care application vendors, many provider organizations are satisfied making this user experience tradeoff in order to securely meet the demands of an increasingly mobile clinical workforce.

WHAT IT MEANS

LAY THE SECURITY GROUNDWORK FOR FUTURE HEALTHCARE MOBILITY TRENDS

As clinical digitalization matures, the privacy and security regulations, best practices, and tools within medical-grade mobility will keep the healthcare provider's BT legal, strategy, and clinical teams busy, both innovating to enhance the working experience of care givers and to ensure that patient information is safe from theft and tampering. In this age of employee mobility, ensuring that the clinical workforce has the proper medical-grade mobile tools to do their jobs must be the guiding principle throughout every BT role. Security perspectives must be solicited from all stakeholders to build the right set of policies and roll out the right tools with the right security infrastructure to support them. It is clear that mobile tools for the workforce will soon be table stakes for hospitals and ambulatory practices. They will need full functionality to both recruit top talent and make the patient population feel that their care givers are properly supported in today's technology climate. Those institutions that do not press hard to have their workforce mobile-ready will suffer over the long term, both from a competitive and security standpoint.

SUPPLEMENTAL MATERIAL

Survey Methodology

Forrester conducted a mixed methodology phone and online survey, fielded in April and May 2014, of 3,305 business and technology decision-makers located in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Each calendar year, Forrester's Business Technographics® fields business-to-business technology studies in 10 countries spanning North America, Latin America, Europe, and Asia Pacific. For quality control, we carefully screen respondents according to job title and function. Forrester's Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Additionally, we set quotas for company size (number of employees) and industry as a means of controlling the data distribution and establishing alignment with IT spend calculated by Forrester analysts. Business Technographics uses only superior data sources and advanced data-cleaning techniques to ensure the highest data quality.

ENDNOTES

[1] Source: Forrester's Business Technographics® Global Security Survey, 2014.

[2] The increasing regulations are in response to the ever-increasing data breaches that affected not only organizations but their customers. For more information on the cost of data breaches within healthcare organizations, see the September 4, 2014, "Brief: Stolen And Lost Devices Are Putting Personal Healthcare Information At Risk" report.

[3] Employee devices are an especially vulnerable conduit for data loss, but in this respect, healthcare is in a class by itself. Since 2005, device loss/theft accounts for 15% of all publicly reported breached records originating from organizations from all industries. However, when looking at only the healthcare industry and healthcare records, this percentage skyrockets to 78%. Source: CyberFactors (http://cyberfactors.com/).

[4] Due to the limited budgets for IT security teams within US healthcare providers, there has been a notable gap in securing private patient data. With an increase in new breaches and regulatory fines, US healthcare providers need to reassess their budgets and effectively prioritize the IT security needs and challenges to improve overall data security. For more information on the OCR's audit activities, see the February 19, 2014, "Industry Spotlight: US Healthcare Security Budgets, Priorities, And Challenges" report.

[5] Source: "Data Breach Results in $4.8 Million HIPAA Settlements," US Department of Health & Human Services (http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/jointbreach-agreement.html).

[6] According to an HIMSS study of 170 mobile technology decision-makers within healthcare provider organizations, 28% felt increased clinician access to mobile technology led to better patient safety. Source: "HIMSS Analytics 2013 Mobile Technology Survey Examines mHealth Landscape," Healthcare Information and Management Systems Society, February 26, 2014 (http://www.himss.org/News/NewsDetail.aspx?ItemNumber=28628).

[7] The mobile mind shift is disrupting the way businesses interact with their customers. Forrester suggests that businesses reassess their current business tactics and undertake the "IDEA cycle" to identify mobile moments; design the mobile engagement; engineer your platforms, processes, and people for mobile; and analyze results to monitor performance and improve outcomes. For more information on mobile moments and how to organize your mobile strategy around these, see the January 24, 2014, "Re-Engineer Your Business For Mobile Moments" report.

[8] Mobile applications are definitely keeping customers engaged and active in an organization's business, but without the proper authentication processes and technologies, it will be difficult to ensure your customers' safety against malicious attacks or fraudulent activities to their personal data. For more information, see the September 17, 2014, "Transform And Protect Your Customers' Mobile Moments With Seamless Authentication" report.

[9] In order to have a seamless mobile engagement, Forrester suggests that S&R pros look to building an effective staff across various areas of expertise, including security architecture, application development and delivery, enterprise architecture, and sourcing and vendor management. For more information on how to build a mobile security team centered on the needs of the business, see the March 14, 2014, "Enable Mobile Engagement Through A Cross-Functional Mobile Security Team" report.

[10] Forrester has assessed several current and emerging technologies for S&R pros who are in the process of assessing new mobile security trends. For a more thorough list of all mobile management and security technologies available to BT professionals, see the December 13, 2013, "TechRadar™: Enterprise Mobile Security, Q4 2013" report.

[11] There is a new shift from containerization to application-wrapping within the enterprise mobility strategy. The shift to application-wrapping will create a more seamless end user experience for your employees. For more information about mobile security, see the July 7, 2014, "In The Mobile Security Bout Of The Year, App Wrapping Beats Containerization On Points" report.

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals