Best Practices For Securing And Empowering A Mobile Workforce

Support Employee Flexibility By Decoupling Security From The Device

by Christian Kane and Chris Sherman

August 17, 2016

Why Read This Report

Companies launch small bring-your-own-device (BYOD) deployments, but these programs often stall when they expand to include both a larger percentage of the workforce and more corporate apps and data access. It's clear that BYOD is here to stay. The role of the security team is to support, even accelerate, this trend, by decoupling security from the device to enable a workforce that wants to use personal devices and apps to aid customers. We spoke with Forrester clients to collect best practices for securing and empowering your mobile workforce.

Key Takeaways

Location, Access To Sensitive Data, And Job Function Affect BYOD Eligibility And Policy
To build a BYOD strategy that is more in tune with how employees work, both operations and security professionals must understand what the needs are for the varying jobs across their workforce. This includes who your employees are, where they work, what tools they use, and what data they access. Security controls must be applied dynamically based on device risk posture.

Take Into Account The Risk Levels Associated With Employee Segments And Device Posture
These include metrics such as sensitivity of data accessible from the device, employee job function, and device security compliance status.

Best Practices For Securing And Empowering A Mobile Workforce

Support Employee Flexibility By Decoupling Security From The Device

by Christian Kane and Chris Sherman
with Stephanie Balaouras, Christopher McClean, Salvatore Schiano, and Peggy Dostie

August 17, 2016

Table Of Contents

2 **Security Teams Must Empower A Mobile Workforce**

Security Pros Must Expand BYOD Use Cases And Ecosystems . . .

. . . While Balancing Security With Employee Experience

4 **Use Forrester's Risk Continuum To Guide Mobile Security Policy**

Location, Access To Sensitive Data, And Job Function Affect BYOD Eligibility And Policy

Use Technology To Decouple Security From The Device

Evolve Your Processes And Policies As Use Cases And Risks Evolve

Recommendations

8 **Use Policy To Cover Your Bases**

10 **Supplemental Material**

Notes & Resources

In developing this report, Forrester drew from a wealth of analyst experience, insight, and research through advisory and inquiry discussions with end users, vendors, and regulators across industry sectors.

Related Research Documents

Building The Business Case For A Bring-Your-Own-Device (BYOD) Program

Develop Mobile Security Metrics With Forrester's Tech Management Balanced Scorecard

TechRadar™: Mobile Security, Q1 2016

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

© 2016 Forrester Research, Inc. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. Unauthorized copying or distributing is a violation of copyright law. Citations@forrester.com or +1 866-367-7378

Security Teams Must Empower A Mobile Workforce

The rise of Millennials in the workforce, increasing employee demand for technology flexibility, and a focus on the employee experience continue to disrupt traditional work procedures. According to our surveys, 70% of information workers use a smartphone at least weekly for work, while 35% say the same about a tablet. And for those who use a smartphone at least weekly for work, 49% chose the device themselves as opposed to following a company-approved list or using a company-issued phone.[1] It's clear that BYOD is the norm, not the exception. The role of the security team is to support, even accelerate, this trend, by decoupling security from the device to enable a workforce that wants to use personal devices and apps to aid customers.

Security Pros Must Expand BYOD Use Cases And Ecosystems . . .

Employee productivity is dependent on access to CRM, collaboration, ERP, and other business apps. If employees can't securely access what they need to do their jobs, they'll find an alternative (and likely less secure) method to do so. Therefore, it's imperative that security pros:

- **Make more apps, devices, and connections available for BYOD.** BYOD programs encompass a wide range of devices, from smartphones to laptops, and each employee requires access to different apps, connections, and services. Managers want access to workflows, the Millennial workforce desires new communication apps, and contractors need access to the protected network — all from their own device. A one-size-fits-all approach to BYOD security will not suffice. BYOD security must be dynamic: Those who take another route will risk employee productivity and satisfaction and clashes with device management pros.[2]
- **Enable more workers with access to BYOD programs.** Every company we spoke with for this report said they are planning to offer BYOD to more employees across the globe. From our experience, once offered, uptake for BYOD programs gains momentum quickly. But each new group added to a BYOD program has its own requirements that the security team must consider, such as regional laws, regulatory obligations, and the context of that employee's work, such as location and sensitive data access. You need to analyze all of these requirements to decide if and how the company can extend BYOD access to more groups.

. . . While Balancing Security With Employee Experience

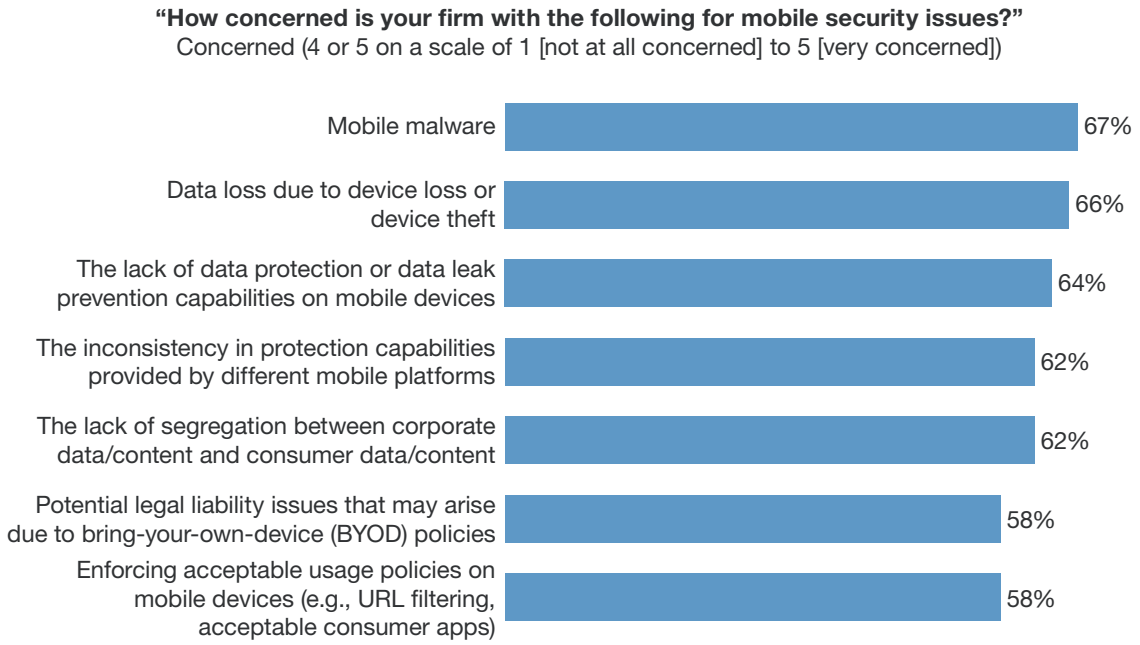
Many companies launch small BYOD deployments, but these programs often stall when they expand to include both a larger percentage of the workforce and more corporate apps and data access. This is because security professionals still have significant concerns about mobile security (see Figure 1). To address these concerns, many security teams implement security tools, but these can often damage the employee experience and productivity. Unsuccessful BYOD programs fail to:

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

- **Address the risks that come with a broader attack surface.** Employees will demand access to sensitive corporate resources from their personal devices, and many operations teams allow a range of device types and OSes onto their corporate network. However, for a BYOD program to be successful, the security team must get involved early and help identify all the new vectors an attacker could use to gain a foothold in the network once the BYOD program is rolled out.
- **Take employee experience into consideration.** Workers want technology to help them get their job done. If they feel like getting access to an app or piece of data is a hindrance or that a secure app is cumbersome, they'll actively look for alternatives from other sources and circumvent the security process. Security and user experience don't have to be at odds if done right.[3] For example, setting individual passwords for each mobile app creates a poor user experience, but single sign-on (SSO) for corporate apps will help employees stay in a state of flow.[4] Security teams must actively engage with business units and individual employees in trials to ensure that security controls don't disproportionately affect employee experience.
- **Understand the mobile requirements of your workforce.** Many security professionals struggle with implementing comprehensive BYOD programs because of the risk associated with securing each operating systems. For example, some companies don't support Android in their BYOD programs because of security concerns. However, given the prevalence of Android worldwide, these practices likely block a large chunk of the workforce from access to BYOD programs. This stalls many BYOD program expansions and will frustrate business users who want access. To overcome this, security professionals must understand the current technology adoption and preferences of the workforce.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 1 Mobile Security Issues Concern Global Security Decision-Makers



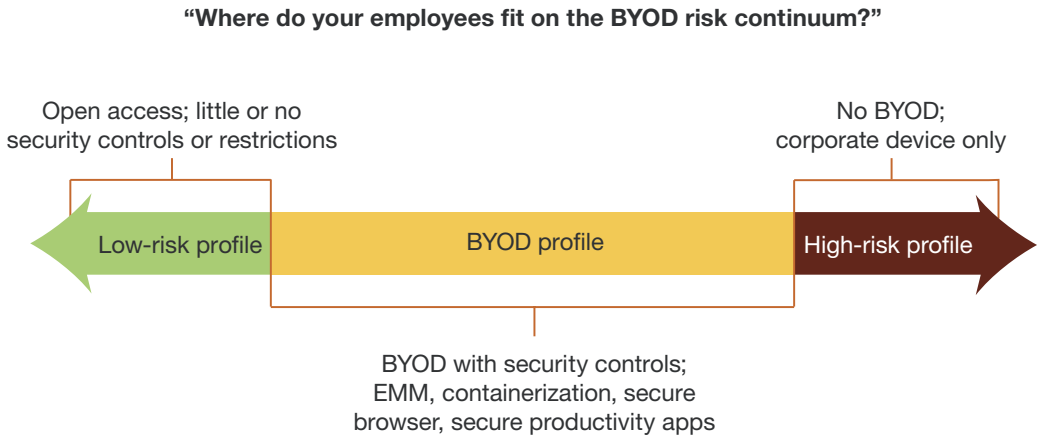
Source: Forrester's Global Business Technographics® Security Survey, 2015

Use Forrester's Risk Continuum To Guide Mobile Security Policy

Successful BYOD programs are created by cross-functional groups that include workers, business leaders, HR, and finance alongside security professionals. Why? Because in order to balance security and user experience requirements, all groups must be represented. This team will create the structure of the program that includes employee eligibility, the technology to allow secure productivity, and the policies and process. To determine for which employees BYOD makes sense, the cross-functional team must perform workforce segmentation projects that analyze the location, access to sensitive information, compliance requirements, and productivity needs of workers.[5] This will place them on a risk scale to determine their BYOD access (see Figure 2).

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 2 Forrester's BYOD Risk Continuum



Location, Access To Sensitive Data, And Job Function Affect BYOD Eligibility And Policy

To build a BYOD strategy that is more in tune with how employees work, both operations and security professionals must understand what the needs are for the varying jobs across their workforce. In collaboration with HR, it's not uncommon for these teams to lead exercises to develop employee personas. In our work helping clients develop personas for their workforce, we've found that the exercise is valuable to help you understand who your employees are, where they work, what tools they use, and what data they access. These factors will help determine if an employee should have access to the BYOD program and to what extent. When analyzing your workforce for BYOD, you should:

- **Decide which locations will offer BYOD.** To create an effective BYOD program, you must start with understanding what your employees work on and the risks associated with bringing this work outside of the office. If your employees are allowed to work with customers' personal identifiable information (PII), you may choose to only allow BYOD access within certain countries where you know you are compliant with all local and regional data privacy laws. For instance, one large international bank we spoke with told us they only offer BYOD in North America and if the employee's job function requires it. Furthermore, certain facilities are more likely to work with sensitive intellectual property due to the nature of their business; in these cases, you may choose to allow BYOD access only while employees are in their assigned local office.
- **Identify who has access to sensitive data.** To ensure that the appropriate levels of security are in place, your BYOD policy must take into account the sensitivity of the data employees use for their specific roles. This starts with defining and classifying your data; Forrester recommends that you adopt our simplified data classification model as you are developing your BYOD policy.[6] This model uses just three levels of data classification: public, toxic, and radioactive. By classifying data according to the way you will protect it, you can more effectively quantify and control the risks associated with BYOD deployment.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

- **Understand the individual job requirements of each role.** An employee's job function is a significant factor for determining BYOD access. Many security teams target a specific role to start with, like marketing or general management, and expand to others. You might exempt certain roles for security or experience reasons. For example, many firms purchase devices for customer-facing roles like retail sales or field service. Because these employees deal directly with customers, the firm wants to maintain a consistent experience for both employees and the customers during their interactions. Firms often exclude hourly workers because of the complexities of calculating overtime. One large financial services company reported: "One concern with hourly workers is overtime work — if they have BYOD with access to email, how do we monitor and limit the hours they work for us?"

Use Technology To Decouple Security From The Device

Security technology can influence user experience and productivity significantly. Therefore, the choices you make here will be critical to the success of the BYOD program. Due to privacy concerns, many security teams are investing in tools that help them isolate and manage corporate data and resources while still providing as close to a consumer experience as possible.[7] This technology includes device and app containers, network gateways, secure browsers, and secure productivity tools. Many of the companies that we spoke with used:

- **Containers to separate corporate and personal apps and content.** Many companies we spoke with only allowed BYOD access via a secure container on the device.[8] They do this for both security of corporate data and employee privacy. One European financial services organization told us they only deploy a secure container to BYOD devices because they don't want to take on any risk related to employees' personal information. However, if the experience with the container is poor, users will just circumvent it. Most enterprise mobile management (EMM) solutions offer multiple container options. Make sure you test the container experience with the end users to make sure you're deploying a container that won't hurt their experience.
- **Secure productivity apps for content and notes.** The first applications that employees want access to are productivity apps like email, calendar, notes, and office tools. Given that these tools also handle a significant amount of corporate data, many security pros have reservations about allowing employees to use the built-in apps or consumer apps for work purposes. Many companies we spoke with opted to use the secure email, file sync-and-share, and productivity tools offered and integrated into their EMM system.[9] These apps allow them to enforce security policies for apps and data but provide an employee-friendly experience.
- **Secure browsers for cloud and corporate data access.** BYOD access shouldn't be restricted to just native apps, however; allowing those devices onto the corporate network or allowing employees to use their device's native browser to access cloud apps and intranet content isn't ideal. Many of the companies we spoke with will use a specific secure browser provided by their EMM solution and require the employee to use this browser to access any company resources that

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

are cloud-hosted or only available via web. This separates their web use for work tasks from their personal browsing, and it gives employees on mobile devices access to company resources that might not have native mobile apps available yet, such as corporate intranet sites.

- **Network access controls for secure connectivity.** Many companies have different segments of their network for different device types or users. The mobility lead at a large manufacturing company told us, "We have three different networks: one for PCs, one for guests, and another for mobile with an integrated NAC component there." With EMM installed on the device and integration with NAC solutions, EMM solutions should be the primary mechanism to dictate the overall usage and access policy, feeding that information to the NAC solution so that when the device connects, the network can wrap the same policies around the connection and traffic. Even though the network is secondary in the policy chain, the network team should be involved. The team needs to understand what policies are being created, provide feedback on what the network can accomplish, and formulate a plan on how the NAC system carries out the policies.

Evolve Your Processes And Policies As Use Cases And Risks Evolve

A BYOD policy is not something you set and forget; you must constantly evolve the strategy as new use cases, devices, and employee demands arise. The policies you put in place for your BYOD program should help you put up some guardrails around these changing requirements and help employees understand what they can and can't do within the program. From our interviews, four best practices emerged:

- **Document all your device and OS restrictions.** Overall, your goal should be to support all of the devices and platforms that employees use. However, new devices and many OS versions can make achieving this goal more difficult. When new devices like wearables enter the environment, make sure you have a plan for evaluating your ability to manage them with your EMM solution. Determining OS version support is more complicated, especially in the case of Android. Many firms hold off on Android support because of the version fragmentation across all of their employee devices. For most, the path forward is to set a minimum supported version based on the security tools required in your organization. For instance, many companies will only support Android 4.4 and above or any version of Android that supports Android for Work containerization.
- **Dynamically evaluate and control device risk.** Your BYOD policies must take into account the risk levels associated with employee segments and device posture. These include metrics such as sensitivity of data accessible from the device, employee job function, and device security compliance status.[10] Ultimately, your mitigation measures should be applied dynamically based on policy and real-time device risk level.
- **Address device retirement, loss/theft, and migration within your BYOD policy.** Have a clear procedure in place to address employees who leave the company, change their device, or whose device is lost or stolen. For employees leaving the company, this might be as simple as taking action to unenroll the device via the EMM solution. Make sure there is a process in place for HR to

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

report employees who leave in a timely manner, as many ops managers say they are not informed about employee departures until weeks or even months later. For lost/stolen devices, there must be a clear procedure for timely reporting and the actions that operations will take — like remotely wiping corporate data from the device or reporting any potential data loss.

› **Ensure all compliance mandates are followed.** For compliance, focus on regional- or country-specific regulations (e.g., hands-free headsets are required while driving) and any vertical-specific regulations (e.g., HIPAA, PCI). The policy must clearly state what actions you'll take if an infraction takes place. This could be anything from removal of access to confiscation of the device in the case of a legal issue. Identify these scenarios for employees and communicate why compliance is important.

Recommendations

Use Policy To Cover Your Bases

Today's workers need the flexibility to meet their job demands with the devices that best fit the context of their work. They also need the consistency of tools and data so that whatever device they choose has the apps and content they need to complete their tasks. When the security team embraces workforce enablement and flexibility as their own desired outcome, this positions them as a productivity enabler rather than a team that employees must fight with or circumvent to get their work done. Your policy and supporting technologies should all drive an integrated strategy to allow flexible workstyles with as few limitations as possible (e.g., we support mobile devices versus we support only iOS devices). BYOD is a critical part of this strategy, even if it doesn't make sense for all employees. As you're creating and refining your BYOD strategy remember to:

› **Construct a policy with a clear understanding of compliance requirements.** In the face of a mandate to act, but with limited visibility into all of the factors affecting BYOD decisions, there is a natural tendency to simply layer on more security controls (with little added benefit) to compensate for unknown risks. Your role is to help foster safe behaviors, control information access, and verify ongoing compliance — all without hampering creativity, productivity, collaboration, or other daily activities.

› **Ensure that policy covers everything that falls outside of your control.** The prospect of personal or nonstandard devices on company networks can pose difficult legal challenges if you don't set expectations upfront, particularly in the European Union. Organizations allowing personally owned devices should require employees to turn over their devices in the event of a legitimate investigation. For example, the US Department of Defense (DoD) allows employees to use a personal BlackBerry device in certain cases, provided they agree to "forfeit the BlackBerry when security incidents occur and to follow all required security procedures and install required software in order to protect the DoD network."

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

› **Require employees to understand and agree to the policy upfront.** The overriding goal of the workforce enablement policy is to protect the integrity of the private and confidential customer and business data that resides on the device. The policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where unsanctioned resources can potentially access it. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to the company's public image. Thus, all employees, contractors, and partners must agree to company-defined processes and regulations before getting access to corporate resources.

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iPhone® and iPad®
Stay ahead of your competition no matter where you are.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Supplemental Material

Survey Methodology

Forrester's Global Business Technographics® Telecommunications And Mobility Workforce Survey, 2016 was fielded between October and December 2015. This online survey included 7,342 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester's Business Technographics ensures that the final survey population only includes information workers who use a connected device for work at least 1 hour per day. ResearchNow fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Forrester's Global Business Technographics Security Survey, 2015 is an online survey fielded in April through June 2015 of 3,543 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.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester's Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

Endnotes

[1] Source: Forrester's Global Business Technographics Telecommunications And Mobility Workforce Survey, 2016.

[2] The mobile mind shift is an expectation that an individual can get what he or she wants in their immediate context and moment of need. This shift applies to your customers and your employees. Unfortunately, many security leaders are unprepared to support their enterprise's mobile strategy for customers and employees. They struggle to balance security and privacy concerns with the importance of user experience and the business objectives of the enterprise. In many cases, security leaders are not even a part of the ideation, design, engineering, and analytics of the customer-facing mobile strategy; instead, they focus myopically on BYOD and lose the opportunity to champion both customer security and customer experience. For more information, see the "Secure And Protect Mobile Moments" Forrester report.

[3] Security leaders must realize that human factors contribute to the success of a security control as much as the risk reduction of the security control itself. Security leaders who choose to ignore human factors run the risk of user security mistakes and even a full security breach. There are three human factors that contribute to the success of a security control and six human factors that act as resistors to effectiveness. To learn more, see the "Raise The Security Bar With Human-Factor-Friendly Design Concepts" Forrester report.

[4] Psychological and neurological research offer critical insights into where high performance and creativity come from, how they make an impact on customer experience and profit, and how organizations are destroying performance without knowing it. With this research, we'll show infrastructure and operations (I&O) pros how to forge a new workforce enablement path and supercharge knowledge workers' productivity and company performance. For more information, see the "Workforce Enablement Defined: Elevate Productivity And Engagement" Forrester report.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

[5] As security leaders look to support the business' engagement with customers, partners, and employees through mobile applications, they often discover gaps in their team's skills and expertise. Successful security executives are building mobile security teams that span multiple IT functions. In many organizations, they also divide core mobile security responsibilities among existing security operations and architecture roles. For more information, see the "Build A Cross-Functional Mobile Security Team" Forrester report.

[6] Defining data via data discovery and classification is an often overlooked, but critical, component of data security and privacy. Security and risk (S&R) pros can't expect to adequately protect data if they don't have knowledge about what data exists, where it resides, how valuable it is to the firm, and who can use it. To learn more, see the "Rethinking Data Discovery And Data Classification Strategies" Forrester report.

[7] Security is behind the curve when it comes to the mobile mind shift. The speed at which employees have adopted mobile applications and pushed them into the enterprise has resulted in a dire need for security and risk (S&R) pros to revamp how they approach mobile security in internal and consumer-facing mobile apps. The time when security and development teams could play the role of curmudgeon by locking down mobile apps has passed. Security and development teams must work together with designers and user experience professionals to embrace the value of mobile moments and provide security that allows the new mobile mind shift to take place. For more information, see the "The Future Of Mobile Security: Securing The Mobile Moment" Forrester report.

[8] As enterprise mobility strategies have shifted from simple bring-your-own-device (BYOD) support to the rapid enablement of a digital workforce, mobile security strategies have naturally shifted from a focus on securing the device itself to securing the sanctioned and unsanctioned mobile applications that employees use to best win, serve, and retain customers. Today, an effective mobile security strategy must prioritize the security of the dozens, even hundreds of mobile applications in use in the enterprise. Two of the most popular solutions, application wrapping and containerization, provide different approaches to mobile application security, and they each offer very different employee experiences and results. For more information, see the "In The Mobile Security Bout Of The Year, App Wrapping Beats Containerization On Points" Forrester report.

[9] In September 2014, we published The Forrester Wave™: Enterprise Mobile Management, Q3 2014, which evaluated 15 vendors using 27 criteria. Our findings showed how well each vendor met the breadth and depth of market demands and where each stood out, helping infrastructure and operations (I&O) and security and risk (S&R) professionals identify the best enterprise mobile management (EMM) solution for their organization. For more information, see the "Market Update: Security Remains A Key Component To Enterprise Mobile Management" Forrester report.

[10] Leading technology management organizations use Kaplan and Norton's Balanced Scorecard (BSC) as a framework for measuring performance and for selecting metrics that demonstrate business value. Forrester's Technology Management Balanced Scorecard revises the original BSC in order to help CIOs measure the performance of their traditional IT as well as their business technology (BT) — the technology, systems, and processes to win, serve, and retain customers. In this report, we outline Forrester's BSC methodology and demonstrate how security and risk (S&R) leaders can apply it to their mobile security strategy and initiatives. To learn more, see the "Develop Mobile Security Metrics With Forrester's Tech Management Balanced Scorecard" Forrester report.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

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 Research (Nasdaq: FORR) is one of the most influential research and advisory firms in the world. We work with business and technology leaders to develop customer-obsessed strategies that drive growth. Through proprietary research, data, custom consulting, exclusive executive peer groups, and events, the Forrester experience is about a singular and powerful purpose: to challenge the thinking of our clients to help them lead change in their organizations. For more information, visit forrester.com.

135284