A Forrester Consulting
Thought Leadership Paper
Commissioned By Dell

October 2016

Is Your IT Security Affecting Your Workforce Productivity?

FORRESTER®

Table Of Contents

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Executive Summary

Every decision of technology leaders within your firm directly or indirectly affects your company's products, services, and ability to win, serve, and retain customers. Your infrastructure and operations (I&O) leaders facilitate autonomy, productivity, and efficiency of workers through various initiatives of mobility, bring-your-own-device (BYOD) programs, and diverse devices and applications in a complex ecosystem. This involves supporting new delivery models and technologies — an approach that Forrester refers to as agile workforce enablement. The technology your firm's employees use every day is an enormous source of personal innovation and competitive advantage. Yet the overwhelming direction of infrastructure I&O pros over the past decade is one of increasing control and narrowing options for employees, in service to auditors and in fear of risk.

Agile workforce enablement is defined as a deeper understanding of workforce experiences built on virtual and cloud technology and combined with updated processes and enhanced self-service to transform employee engagement and workstyle flexibility.

Business leaders look to invest in employee initiatives to bring in more flexibility and boost employee productivity and creativity. As a result, BYOD and freedom to choose your own device will become an important tool not only to enhance employee experience but also to foster innovation and meet rising customer expectations. The era of single OS, single device is gone, and you must make peace with the reality of the technology-diverse world. But BYOD programs bring several security challenges through the complexity they introduce in the technology landscape, especially when the workforce demands access to diverse corporate apps and information flow across various types of devices.[1]

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. To build a workforce enablement 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.

Enterprise endpoint security strategy plays a critical role in closing the gaps for employee productivity and doing so in a way that also improves what are often considered conflicting goals — improving security and lowering costs. There are several critical questions that must be answered to deliver a winning strategy: What are the major threats organizations faces? Where are the major security breaches? Is the current security framework apt? How do I balance productivity, costs, and security requirements? What are the major endpoint security trends and challenges across the Asia Pacific and Japan (APJ) region?

In August 2016, Dell Technologies commissioned Forrester Consulting to evaluate some of the key challenges, drivers, and trends that businesses are facing to ensure workforce security across APJ. To explore this trend, Forrester conducted a custom study to identify key business priorities, challenges, and methods being adopted across industries. The study included in-depth surveys with 327 senior business and technology executives and end user computing decision-makers in China, India, Japan, SEA (Singapore, Malaysia, Indonesia, Philippines), Korea, and ANZ (Australia, New Zealand) within their organizations.

Key Findings

This study yielded a number of key findings:

- **Employee experience and security must go hand in hand for effective workplace security strategy.** Your workforce is exposed to a plethora of options through consumer applications and devices and has grown comfortable with diverse productivity tools and applications. In order to meet your business objectives, your employees should remain productive and engaged, which can be achieved through delivering superior employee experience. Your security team should work in tandem with various functional teams in HR, legal, and compliance to develop a security strategy that not only delivers an improved risk profile but also makes the IT environment more user-friendly.

Enterprise endpoints are not secure. A number of factors, such as a growing number of employee devices and operating systems, lack of adequate remote access management, weak user authentication, and increasing sophistication of device malware, have led to endpoint devices becoming more vulnerable than ever.

- **The complexity of the IT organization leads to multiple security challenges.** Your enterprise ecosystem is growing, and it spreads across the IT infrastructure and business applications of your extended network vendors, suppliers, and business partners. Critical business information flows across several platforms, operating systems, and often devices. Add to this a complex web of consumer and nonconsumer tools and applications that run over an intricate IT environment. Increasingly sophisticated malware is constantly attacking your IT environment, posing multiple security challenges.
- **The latest workforce technology will improve your risk profile.** One way to improve your risk profile is to procure new PC hardware with updated security and compliance measures. Keeping your devices updated will also enhance the overall employee experience, thereby affecting the productivity of the organization.

Everyday Threats Are Evolving With The Evolution Of The Mobile Workforce

For your employees to do their very best work, they need access to a wide range of business applications and sensitive information — often from whatever endpoint device they deem appropriate. They need to remain connected to meet your business objectives, forcing organizations to increase their budgets for mobility solutions. Results from Forrester's Global Business Technographics® Networks And Telecommunications Survey show that 72% of global enterprise telecommunications decision-makers are focused on bolstering mobility support for employees over the next 12 months. In the face of growing complexity due to rising cloud adoption, diverse business apps and operating systems, and rising information flow across business ecosystems, the need for more effective endpoint security controls has never been more apparent.[2]

Endpoint malware has become increasingly sophisticated, affecting numerous large-scale breaches in organizations across all industries and sizes, ranging from mass malware loaded with ransomware (as in the case of CryptoLocker) to targeted in-memory attacks used in conjunction with zero-day application/OS exploits. Unfortunately, adversaries target employee desktops and laptops and use them as a beachhead into the corporate infrastructure where your servers reside. An increasingly mobile workforce and an ever-evolving threat landscape will push organizations to look for more secure endpoint devices and security solutions to guard against the threats that have surpassed traditional antivirus capabilities.[3]

According to our survey, a large chunk of security breaches occur due to internal incidents within the larger ecosystem of the business partner/third-party supplier organization (32%) and within the respondents' own organization (29%), while 30% of security breaches originate from a security breach of an employee's device (see Figure 1). Many of these incidents occur due to malicious insiders taking advantage of a flawed "trusted" approach to security, weak identity and access management control, and poor endpoint security and monitoring. Some of the key highlights are as follows:

- **Increasing use of consumer applications leaves security holes.** The task of protecting corporate data is made particularly challenging when it ends up within third-party file-sync-and-share systems. This was noted

FIGURE 1
Internal Incidents Are The Major Sources Of Security Breaches Across Organizations In APJ

"Which of the following security breaches occurred in the organization over the past 12 months?"
(Select all that apply)

Base: 327 IT and business decision-makers across organizations in China, India, Japan, SEA (Singapore, Malaysia, Indonesia, Philippines), Korea, and ANZ (Australia, New Zealand)

Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, August 2016

by 78% of our survey respondents as a top security concern that is introduced from technology or company initiatives (see Figure 2). Many companies do not have visibility into their corporate data as it travels between emails and consumer apps such as file-sync-and-share tools, adding to data risk through endpoint devices.

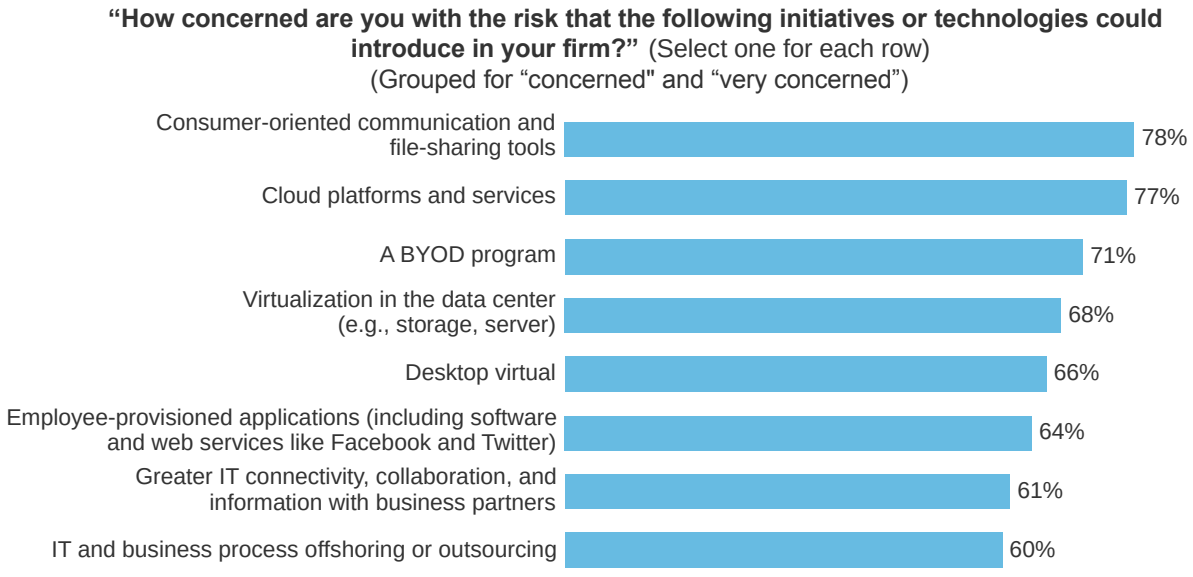
- **Growing cloud adoption adds to security vulnerabilities.** Sensitive data is at risk, whether from enterprise-deployed software-as-a-service (SaaS) applications or information workers bringing their own preferred SaaS services and tools to work with them. Seventy-seven percent of our survey respondents said that they are concerned with the security risk introduced through cloud platforms and services (see Figure 2). There is a high demand for visibility into data movement and use, along with the capability to enforce use and handle policies of data going into and stored in the cloud. Security and risk (S&R) pros are concerned about data security and compliance vulnerabilities with consumer cloud storage solutions.

- **Workforce flexibility adds to the security challenges.** BYOD programs have added complexity to the security landscape through a multiplicity of operating systems, devices, and applications in the business environment, as cited by 71% of our survey respondents (see Figure 2). In certain environments, lack of monitoring and control of corporate and consumer data leaves critical gaps in the security framework. Understanding where corporate data is flowing and applying the appropriate controls is critical to successfully securing the modern workplace.

- **A connected mobile workforce feeds into the increasing security concerns.** A need for remote access and connectivity has become the norm due to the evolving nature of customer and employee expectations. The availability of business applications and productivity tools frees employees to work from any location at any time, thereby increasing their productivity. As the demand for real-time access to information grows across platforms, networks, and devices in absence of consistent security policy framework, so do the security concerns.

FIGURE 2

Growing Demand For Employee Flexibility Through Technology Is The Major Source Of Security Concerns



Base: 327 IT and business decision-makers across organizations in China, India, Japan, SEA (Singapore, Malaysia, Indonesia, Philippines), Korea, and ANZ (Australia, New Zealand)

Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, August 2016

Current IT Security Policies And Control — Are They A Bane Or A Boon?

Technology diversity and changing employee workstyles open the door to a host of security issues that threaten the brand and security of your organization. I&O leaders must create a fine balance between providing flexibility to the employees and managing security risks and avoid creating any unnecessary barriers that would hinder employee experience and productivity.[4]

Increasing adoption of diverse business and consumer technology and use of various end user computing and internet-of-things (IoT) devices have made the static security policy obsolete. More often than not, data security policies are a checkbox item rather than a well-thought-out schema. They not only tie in with the current requirements of information security and privacy policy, enforcement, and auditing activities but also accommodate for future dynamic expansion of endpoint hardware and software diversity.

Availability of diverse tools and devices helps drive better employee engagement and innovation because it gives people in your firm the freedom to choose the tools that work best for them and find better productivity.[5] Concurrently, technology diversity also brings in new security challenges. Respondents to our survey said that the biggest barrier to managing security for the IT organization is complexity (35%) the challenge of maintaining compliance and security effectively as noted by 26% of our survey respondents (see Figure 3). The correct solution is a strategy that brilliantly achieves the conflicting goals of embracing BYOD and consumerization while slashing the risks and costs at the same time. The need for an overhaul in strategy to address existing security challenge has been borne out in the responses to our survey:

- **An effective end user computing security strategy leads to increased workforce productivity.** Employees are continually installing new software and have little tolerance for security products that stand in the way of their productivity. With growing IT environment complexity, the security risk to the end user computing environment increases, as agreed upon by 50% of our survey respondents. Fifty-four

FIGURE 3
Organizational Complexity And BYOD Policies Are The Biggest Barriers To Managing Security Effectively

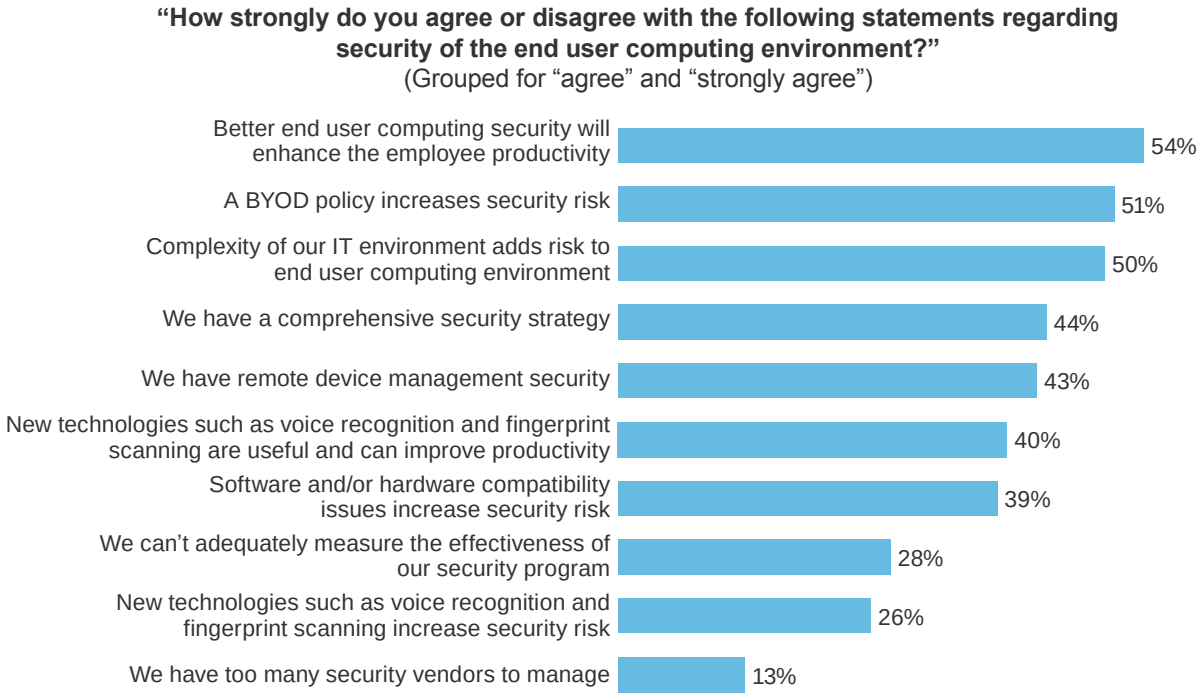
Base: 327 IT and business decision-makers across organizations in China, India, Japan, SEA (Singapore, Malaysia, Indonesia, Philippines), Korea, and ANZ (Australia, New Zealand)

Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, August 2016

percent of the survey respondents also agreed or strongly agreed that better end user computing security does enhance employee productivity (see Figure 4). When choosing any security technology for an employee device, don't underestimate the importance of preserving endpoint performance and user experience.

- **Archaic security policies restrict organizations from giving flexibility to their workforce.** Our global survey for Dell revealed that employees are leveraging multiple different PC devices to support their work activities, and 81% are using a desktop computer. They are also using laptops (71%), smartphones (70%), and tablet computers (40%) for work purposes. Still only 43% of APJ respondents said that they have a remote device management security solution in place. Furthermore, over half (51%) of respondents believe that implementation of BYOD increases security risk in the end user computing environment (see Figure 4).
- **New device authentication technology is still not mature.** New user authentication techniques, such as fingerprint scanning and voice recognition, still leave several easy breakthrough options. Hackers can impersonate using molds for graphing fingerprints and voice recognition attacks to bypass security mechanisms using a cloned speech command. Only 40% of the survey respondents said that these technologies help them improve the productivity of their employees, while 26% of the respondents believe that the same technologies actually increase the security risk of their organization (see Figure 4).
- **Compliance is the biggest device security challenge for BYOD policy.** The global privacy legal landscape is a bumpy and thorny one due to the plethora of privacy laws and the lack of harmonization within and across countries. Seventy-nine percent of our survey respondents said that a potential legal liability that may arise due to BYOD policies is their biggest device security challenge (see Figure 5).

FIGURE 4
Lack Of Security Policy Maturity Leads To Diverse Endpoint Security Challenges



Base: 327 IT and business decision-makers across organizations in China, India, Japan, SEA (Singapore, Malaysia, Indonesia, Philippines), Korea, and ANZ (Australia, New Zealand)

Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, August 2016

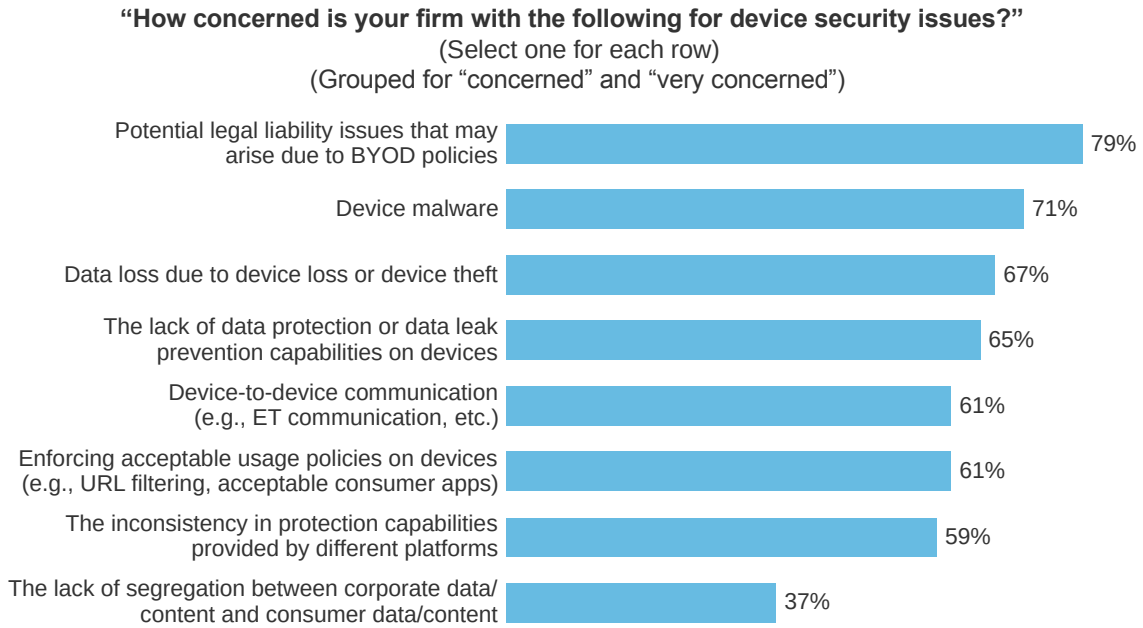
- **Device malware is a major endpoint security threat.** As malware increases in sophistication and the number of new variants and methods of obfuscation rises, antivirus technologies have become less effective at stopping advanced threats to employee endpoints. Seventy-one percent of business and IT leaders of APJ said that device malware is a major concern for their device security, clearly indicating the need for robust and secure antimalware solutions in endpoint strategies (see Figure 5).
- **Complex environments lead to security challenges.** Access to information through various sources within the enterprise ecosystem is one of the most important activities of your information worker.

Since your corporate and consumer information resides in device-to-device communication, it needs to remain secure. Unfortunately, 61% of our survey respondents are very concerned about security risk through device-to-device communication. Another issue arising is the security risk arising from the growing complexity of multiple platforms and operating systems in your IT ecosystem (see Figure 5).

.

.

FIGURE 5
Potential Legal Liabilities And Device Malware Top Device Security Issues



Base: 327 IT and business decision-makers across organizations in China, India, Japan, SEA (Singapore, Malaysia, Indonesia, Philippines), Korea, and ANZ (Australia, New Zealand)

Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, August 2016

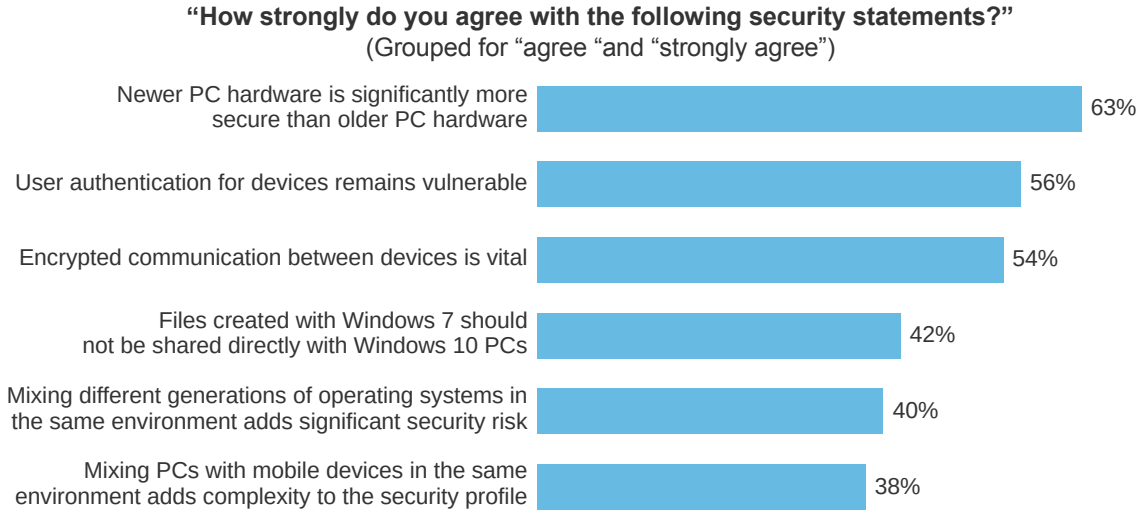
Employee Needs Will Drive The Endpoint Security Strategy

To build an effective device 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. In order to deliver this, organizations need to be more creative while mapping employee needs, organizational productivity, and security requirements. If employees 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. Security teams must actively engage with business units and individual employees in trials to ensure that security controls don't disproportionately affect employee experience. Some key observations from our research are:

- **Procuring new PCs is important.** Nearly two-thirds (63%) of our survey respondents said newer PC hardware is more secure than older PC hardware. Updating to newer hardware will help organizations close the vulnerabilities of user authentication for devices, as suggested by 56% of survey respondents (see Figure 6).
- **Half of the organizations are not secure enough.** Fifty-five percent of our survey respondents said that stronger encryption methodologies will improve the overall risk profile of the company, while 48% of the business and IT decision-makers said that improvement of advanced threat identification techniques will help them reduce the overall security risk within the organization.
- **Improvement of user authentication/advanced threat identification yields several benefits.** Sixty-eight percent of business and IT leaders in APJ said that using these techniques improves management of different operating systems together. Forty percent of the survey respondents said that management of PCs and mobile together becomes easier, while 34% said that user experience improves with an improvement in user authentication and implementation of advanced threat identification/stronger encryption (see Figure 7).

FIGURE 6

Newer PCs Will Improve The Organization's Risk Profile Even As User Authentication And Encryption Pose Significant Challenges

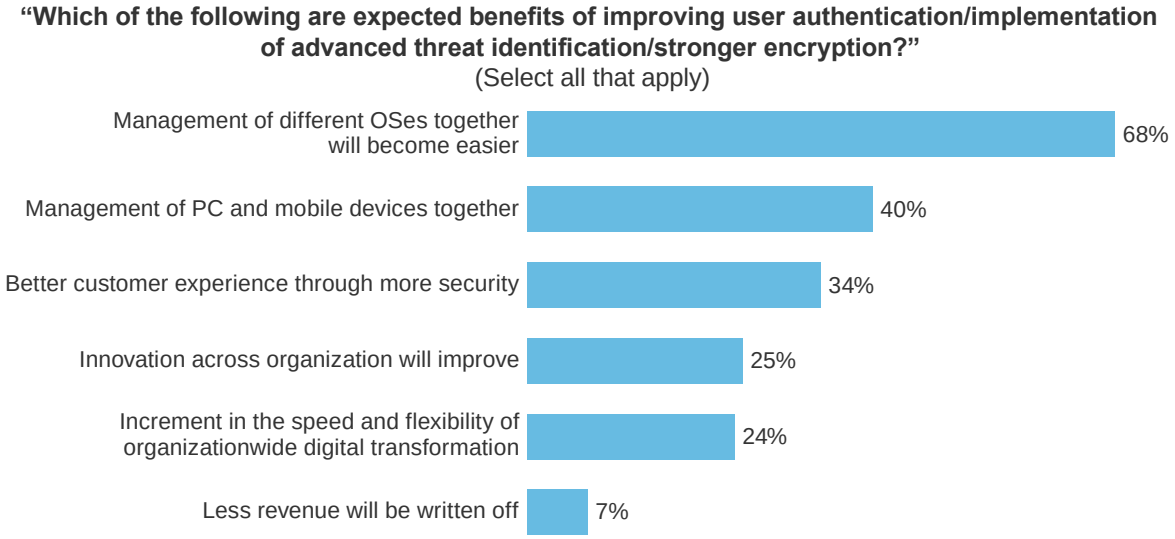


Base: 226 IT and business decision-makers across organizations in China, India, Japan, SEA (Singapore, Malaysia, Indonesia, Philippines), Korea, and ANZ (Australia, New Zealand)

Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, August 2016

FIGURE 7

Improvement In Security Techniques Will Lead To Better Management Of Complex IT Environments



Base: 255 IT and business decision-makers across organizations in China, India, Japan, SEA (Singapore, Malaysia, Indonesia, Philippines), Korea, and ANZ (Australia, New Zealand)

Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, August 2016

Key Recommendations

Successful companies will institutionalize these suggestions to ensure a secure workplace:

- **Become an employee productivity evangelist within your organization.** Remember, the productivity of your organization's workforce is the engine that drives your business. The data is clear that security measures that interfere with employees' ability to get their work done cause them to devise increasingly clever ways to work around them. For every key security decision, consider how it will affect employee productivity and choose the least impactful method that still delivers excellent security.
- **Choose the most secure device hardware.** In general, security measures that operate at the hardware level have the least impact on employee productivity because they're usually transparent to the user while offering superior protection compared with software-only solutions. For example, the Trusted Platform Module (TPM) in commercial-grade PC hardware offers strong encryption to ensure the integrity of the system with no negative impact to the user. Many commercial PCs also offer biometric features that save people time by eliminating the need to type in a password to log in.
- **Make authentication, network, and data security part of your endpoint security strategy.** Secure devices alone are not enough to guarantee information security. A secure endpoint can still be used by malicious insiders to gain unauthorized access to data or do damage. Your strategy must be comprehensive and include not only strong network authentication and access mechanisms, but also monitoring of data flows between endpoints and applications to spot any unexpected or malicious behavior.

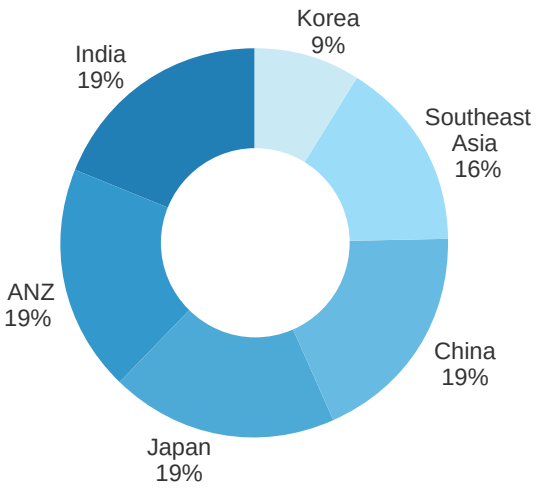
Appendix A: Methodology

In this study, Forrester conducted computer-assisted telephone interviewing (CATI) of 327 IT and business decision-makers across organizations in China, India, Japan, SEA (Singapore, Malaysia, Indonesia, Philippines), Korea, and ANZ (Australia, New Zealand) to evaluate key business trends, growth inhibitors, and innovative solutions for workplace security. Survey participants included decision-makers and business leaders in business or IT roles. The study began in August 2016 and was completed in September 2016.

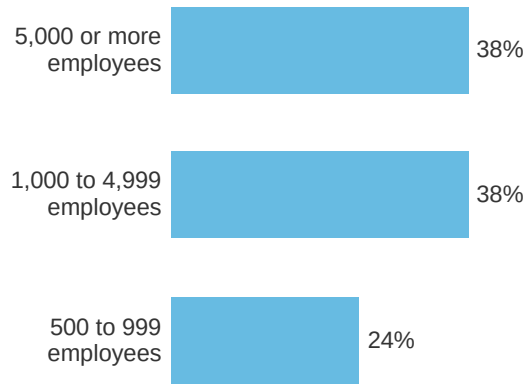
Appendix B: Supplementary Graphs And Demographics

FIGURE 8
Demographics: Company Type — Location And Employee Size

"In which country do you work?"
(Please select one)



"Using your best estimate, how many employees work for your firm/organization worldwide?"
(Please select one)

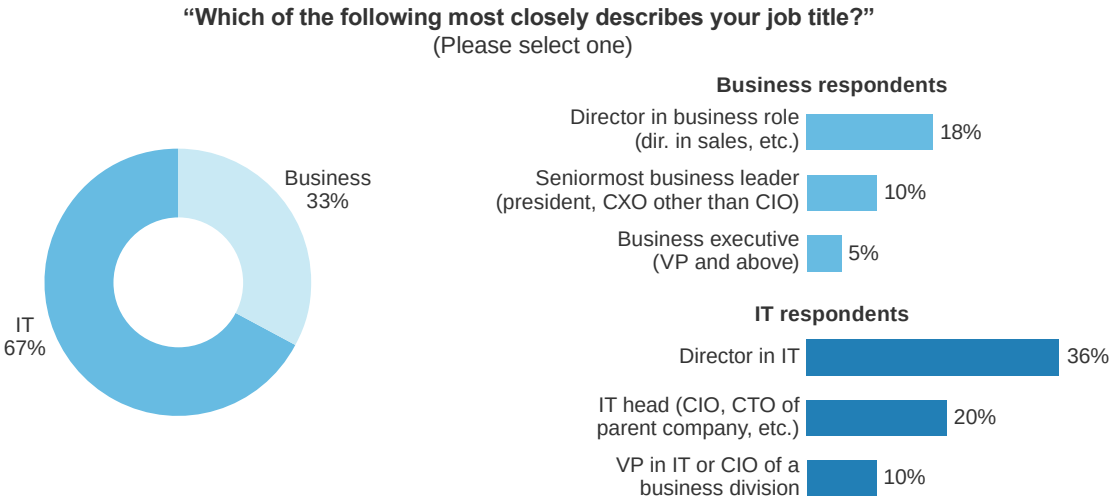


Base: 327 IT and business decision-makers across organizations in China, India, Japan, SEA (Singapore, Malaysia, Indonesia, Philippines), Korea, and ANZ (Australia, New Zealand)

(percentages may not total 100 because of rounding)

Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, August 2016

FIGURE 9
Demographics: Position In Organization

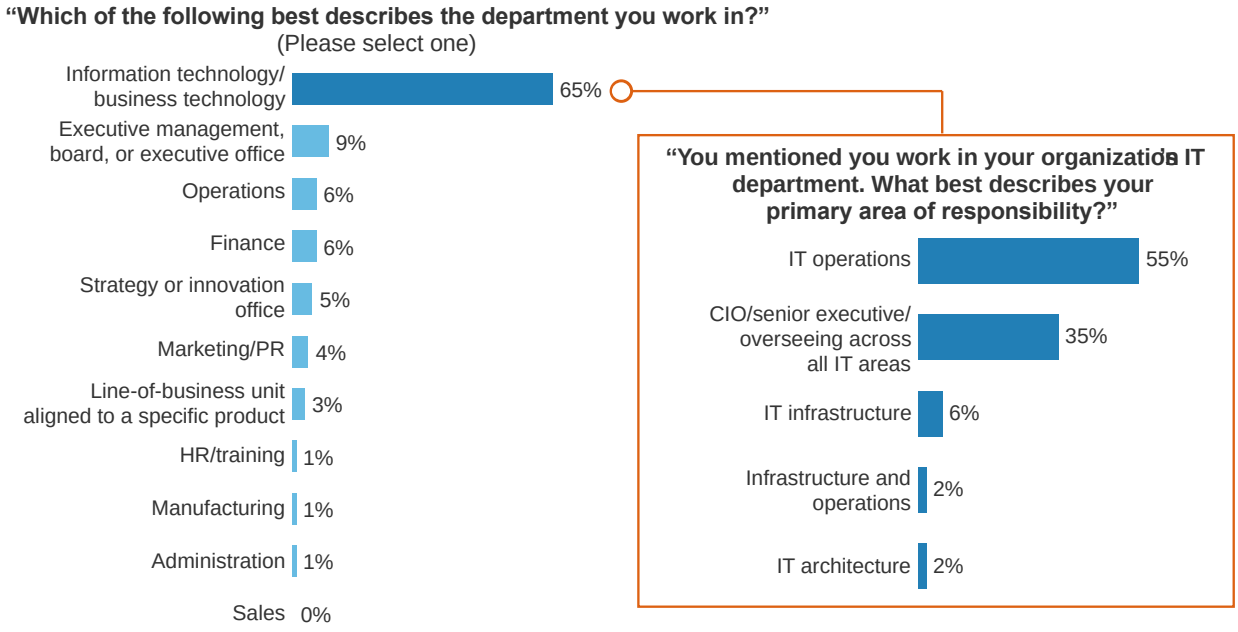


Base: 212 IT and business managers across organizations in the US, the UK, India, Australia, South Africa, Mexico, and Germany

(percentages may not total 100 because of rounding)

Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, August 2016

FIGURE 10
Demographics: Department



• The majority of decision-makers identify themselves with the IT/technology department.

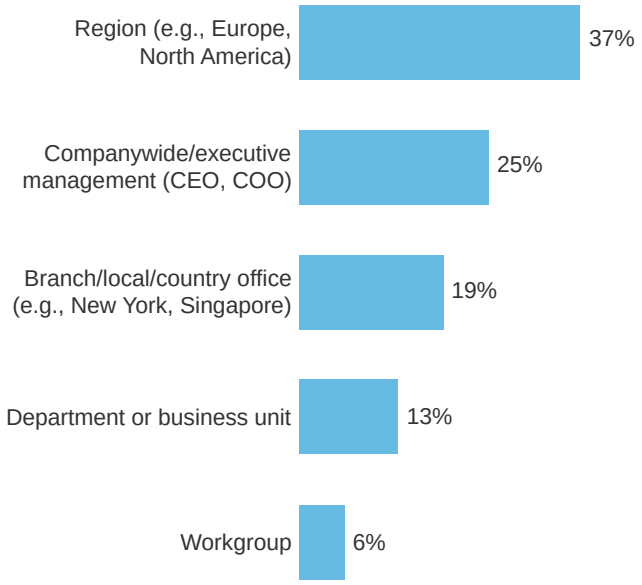
Base: 327 IT and business decision-makers across organizations in China, India, Japan, SEA (Singapore, Malaysia, Indonesia, Philippines), Korea, and ANZ (Australia, New Zealand)

(percentages may not total 100 because of rounding)

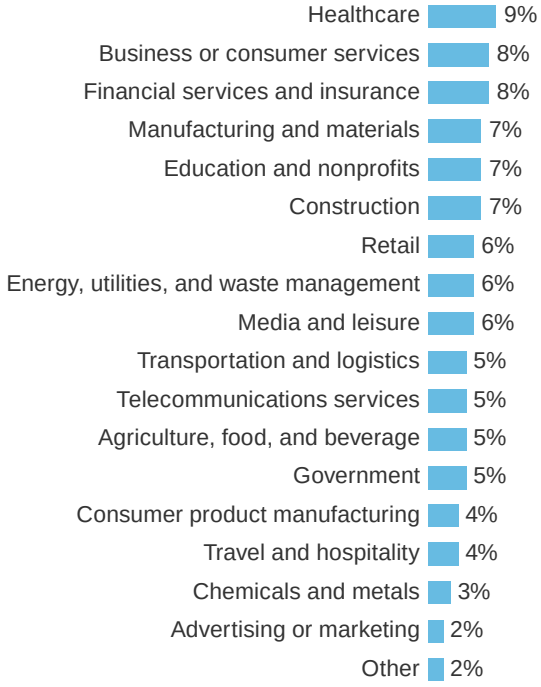
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, August 2016

FIGURE 11
Demographics: Industry And Management Authority

"Which of the following best describes the scope of your management authority?"



"What is the primary industry of your organization?"
(Please select one)

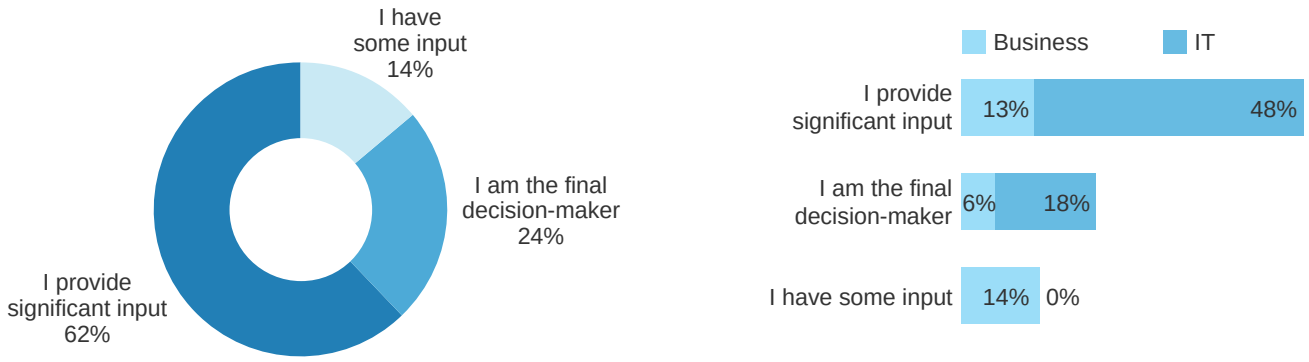


Base: 327 IT and business decision-makers across organizations in China, India, Japan, SEA (Singapore, Malaysia, Indonesia, Philippines), Korea, and ANZ(Australia, New Zealand)

Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, August 2016

FIGURE 12
Demographics: Hardware Procurement Role

"What is your involvement in your organization 's client computing hardware procurement decisions?"



Base: 327 IT and business decision-makers across organizations in China, India, Japan, SEA (Singapore, Malaysia, Indonesia, Philippines), Korea, and ANZ (Australia, New Zealand)

Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, August 2016

Appendix C: Endnotes

[1] Source: “Elevate Human Performance With Workforce Enablement,” Forrester Research, Inc., May 2, 2016.

[2] Source: “Improve Skills And Staffing For A Better Employee Tech Experience,” Forrester Research, Inc., April 4, 2016.

[3] Source: “The 2016 State Of Endpoint Security Adoption,” Forrester Research, Inc., April 25, 2016.

[4] Source: “Best Practices For Securing And Empowering A Mobile Workforce,” Forrester Research, Inc., August 17, 2016.

[5] Source: “Know Your Data To Create Actionable Policy,” Forrester Research, Inc., February 18, 2016.