A Forrester Consulting
Thought Leadership Paper
Commissioned By Dell

November 2019

The Balanced Security Imperative

FORRESTER®

Table Of Contents

Project Director:
Tarun Avasthy,
Market Impact Consultant

Contributing Research:
Forrester's Infrastructure &
Operations research group

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

Balanced security requires firms to transition from treating privacy and data security as compliance requirements to one that champions privacy and uses its technology prowess to differentiate the brand. Any misstep with or changes to the IT infrastructure can and will exacerbate complexity, which is why building a balanced security strategy is so important. A balanced security strategy negates complexity by keeping up with the pace of technological change as well as industry disruption and evolving regulatory compliance.

In March 2019, Dell commissioned Forrester Consulting to evaluate the evolving security trends and technology needed to protect and enable employees. Our study found that empowering employees while adhering to security protocols improves employee productivity. Forrester conducted an online survey of 887 senior business and IT decision makers to explore this topic.

KEY FINDINGS

- **Constantly evolving threats force midmarket firms to be more proactive than reactive.** With many high profile security breaches and/or cyberattacks being reported regularly in the news, midmarket firms must become more forward thinking in their approach to security.
- **Spending on security alone is not the magic bullet.** Midmarket firms must declare a culture of enablement, continuous skills development for employees, and perhaps most critically, a sound and robust security infrastructure.
- **Restrictive IT policies will lead employees to evade IT security best practices, for the sake of getting work done.** Bending the rules is not uncommon in the workplace, but outright avoiding IT policies in order to get work done is risky.

Organizations Require Balanced Security To Boost EX And Operational Efficiency

A diverse technology landscape and changing employee workstyles have opened the door to a host of risks that threaten the overall security posture of an organization and its reputation. A robust, balanced security infrastructure ensures that business performance is maximized and protected. Meanwhile, as a business initiative, employee experience (EX) is growing in importance as more companies are interested in developing a workforce experience strategy that reduces friction and enables employees to complete their most important tasks in an efficient way.

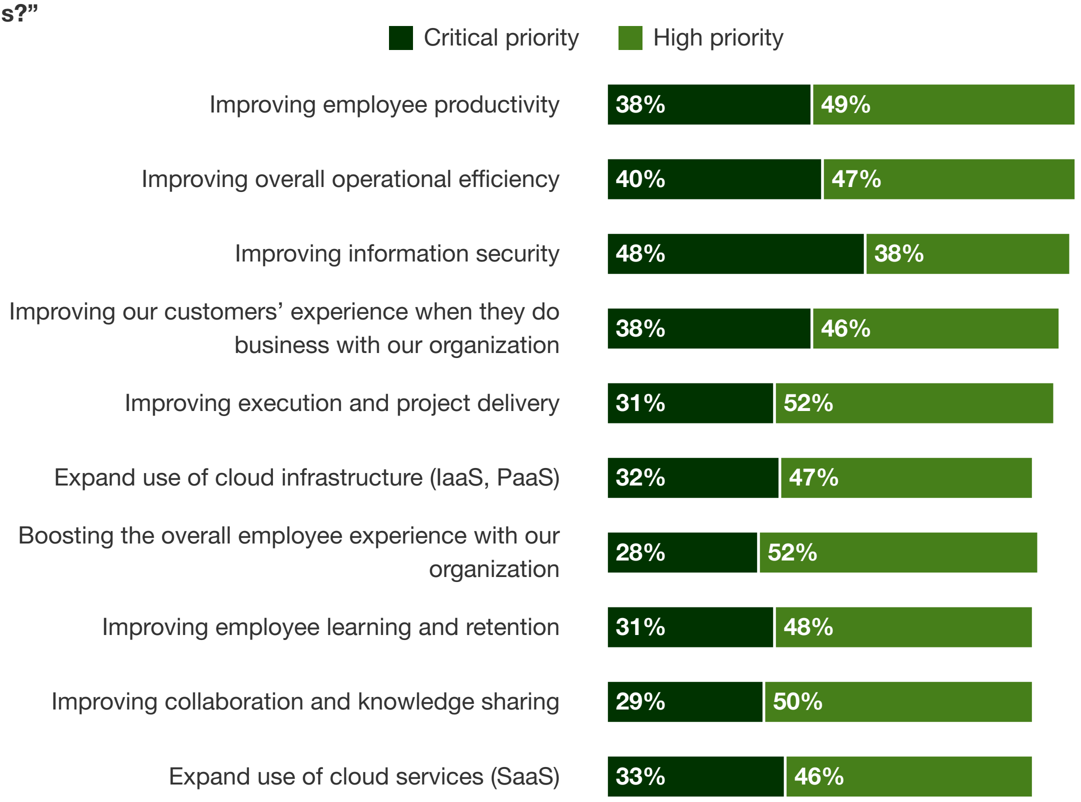
Spending on technology alone will not help to improve the employee experience. Organizations, specifically midmarket firms, must also invest in building a culture of employee enablement, continued skills development, and robust security in order to manage risk while supporting business performance. To deliver a great EX, firms need a balanced approach to security across three key areas (see Figure 1):

- **Increasing the employee's productivity.** Today's busy workplace puts intense cognitive demands on employees, which is why supporting them to achieve mastery over their work is an inherent dimension of high EX. However, many security measures do the opposite and interrupt their productivity levels. With this in mind, midmarket firms are looking to improve the employee's productivity over the next 12 months (88%). As technology continues to evolve, respondents also said they will improve employee retention and learning (79%) — ensuring the talent gaps remain as close as possible.
- **Boosting information security.** In order for employees to be successful, they also need unfettered access to information required to do their jobs, regardless of where they are working from and the devices, they use to get the job done. However, firms are under a barrage of different types of cyberattacks and events that can disrupt business operations and compromise sensitive data — whether it is the personal information of customers/employees or sensitive corporate information. In addition, concerns like third-party risk and supply chain security mean that organizations must expand their view of the risks to the business beyond their own environment. It's no surprise that 86% of firms said they will be prioritizing information security.
- **Improving operational efficiency.** Security teams that underpin business operations need to establish a much more consistent process in how they operate and strive to be proactive rather than reactive in their approach to security. Midmarket firms should move beyond a standard checkbox approach, basing security efforts primarily on compliance requirements, to a more strategic and risk-based approach to security. This requires processes to support risk intelligence, threat identification and response, risk assessment, and business resiliency in order to meet the promise of project execution and delivery (83%).

Midmarket firms should invest in building a culture of employee enablement, continuous skills development, and strive toward a robust security infrastructure.

Figure 1

"Which of the following technology-related initiatives is your department or division prioritizing over the next 12 months?"



Base: 887 business and IT decision makers who are involved in decision making for laptops, computers, and other devices
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, September 2019

Evolving Threats And IT Complexity Are Ongoing Challenges

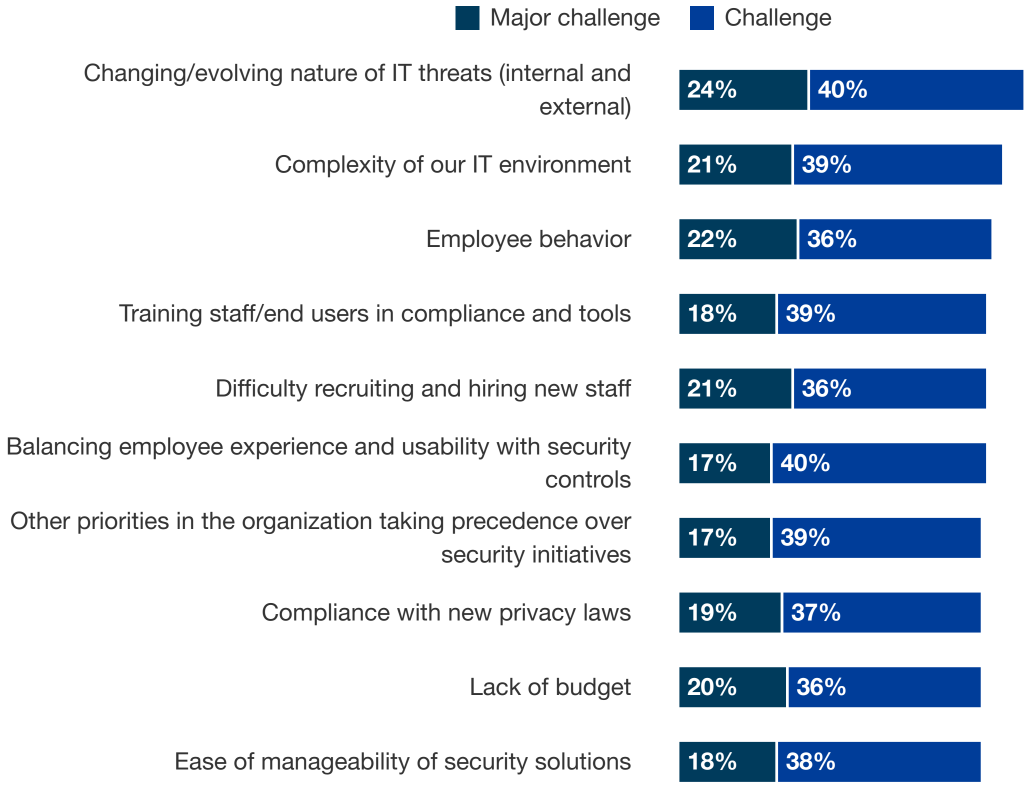
Faced with competing priorities, emerging technologies, and new regulatory requirements, security managers are tasked with continuous defense and making sure that attackers are not successful. However, when we asked survey respondents what the top security challenges are, we found (see Figure 2):

› **The evolving nature of threats keeps midmarket firms alert and in a constant state of playing catch up.** IT must have a robust, adaptable strategy in order to create friction for attackers. Sixty-five percent of organizations face issues with the changing nature of security attacks today. As leaders within the organization see the latest mentions of cyberattacks and events in the news, and then ask if it could happen to your organization, it's useful to assess and communicate the why and how (or why not, based on your environment and controls). However, don't let this reactive approach drive your overall security strategy.

- **IT complexity translates to increased risk and IT management challenges.** Missteps with or changes to the IT infrastructure can and will exacerbate complexity, which is why building a robust security strategy is so important. A security strategy that is able to keep pace with technology change, industry disruption, and evolving regulatory and compliance will serve as a catalyst for positive change. A strategy that enables you to build security from the start is preferable to bolting it on after the fact, as is one that takes a closer look at consolidating the number of security products in your environment to support easier IT management. Currently, 60% of survey respondents view the complexity of their IT environment as a threat to their organization.

Figure 2

"Which of the following are IT security challenges for your organization?"



Base: 887 business and IT decision makers who are involved in decision making for laptops, computers, and other devices
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, September 2019

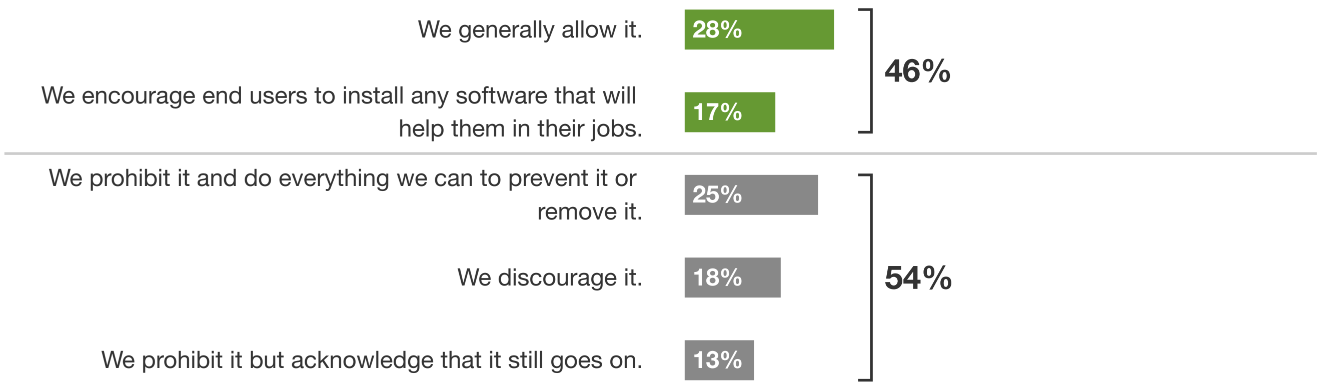
EMPLOYEES NEED TO FEEL EMPOWERED OR THEY WILL CIRCUMVENT IT POLICIES

Employees will choose the path of least resistance in order to get their work done. When employees want to install their own software/applications to help them do that, 54% of respondents from midmarket firms said they prevent, discourage, and prohibit employees from doing so, but they know that it still goes on. Employees need to feel like they are being supported by the business (see Figure 3).

Employees need to do their job in a way that is nondisruptive to their productivity, and security personnel need to ensure the business is protected. Fifty-eight percent of respondent's report that sometimes employees will circumvent IT policies to get their tasks completed, putting the business at risk. This is why it's important to balance EX and usability with security controls, but 57% said this remains a challenge. Furthermore, if organizations cannot measure the effectiveness of their security program (52%) they will be running an unending race, with the finish line – being our golden archway of balanced security strategy – always being just over the next hill.

Figure 3

"For your typical information worker, what is your IT organization's policy for using/installing their own software?"



Base: 887 business and IT decision makers who are involved in decision making for laptops, computers, and other devices
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, September 2019

Your Security Infrastructure Needs To Evolve With The Times

The idea of a corporate perimeter is quaint and outdated today. Employees are working from various locations and require access to information from anywhere. The consumer market is influencing how employees are working in a corporate environment and with what devices. A digital business has no perimeter. Today, your organization can extend into the cloud, support a mobile workforce, digitize physical environments with connectivity via sensors and other internet connected devices. There is an increasing permutation of ways in which both employees can expose sensitive data and attackers can compromise your environment and data. In today's work and threat environment, security strategy and architecture must evolve to become data-centric and rooted in a Zero Trust approach to security.

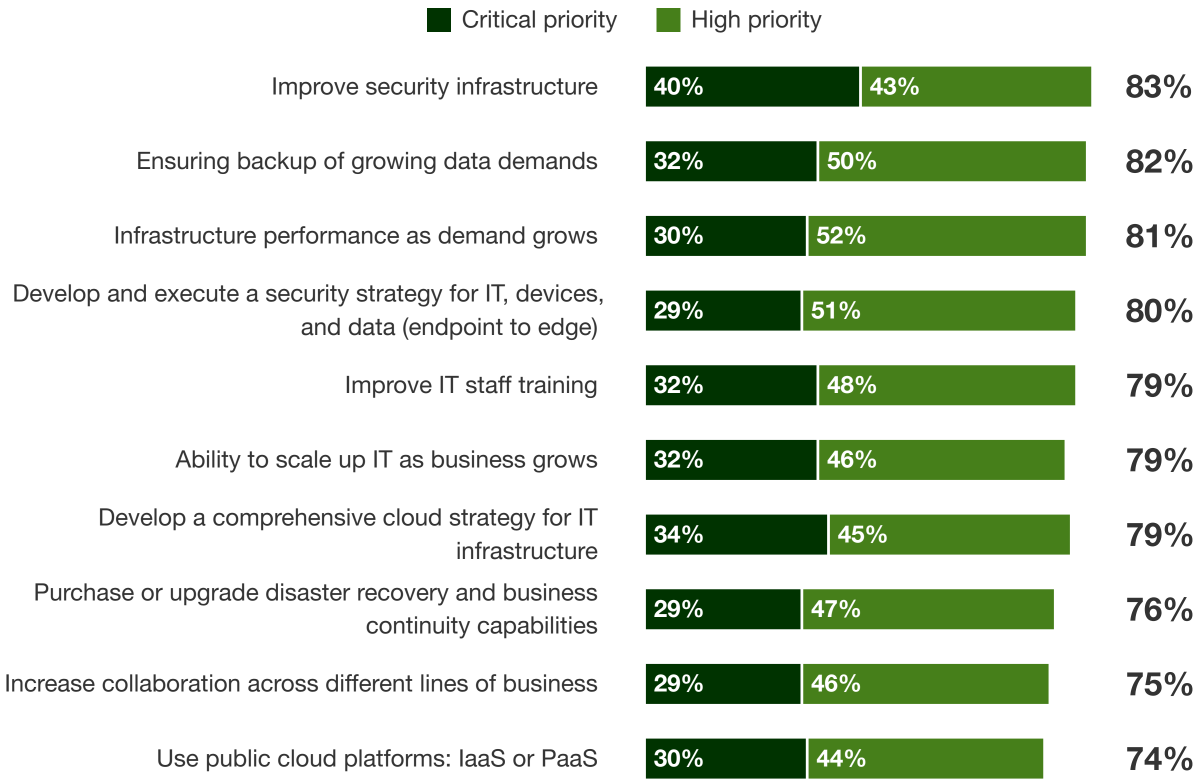
Zero Trust is a conceptual and architectural model for how security teams should redesign networks into secure micro-perimeters, use obfuscation to strengthen data security, limit the risks associated with excessive user privileges, and use analytics and automation to dramatically improve security detection and response. This approach helps to dramatically improve data security. Many organizations today already take a Zero Trust approach. The survey respondents identified the following infrastructure priorities that indicate a readiness for Zero Trust (see Figure 4):

- **Training end users to improve secure data-handling practices.** In order to gain access to intellectual property, attackers will target employees and contractors. At work, employees are using connected devices which interact with cloud services on corporate-owned systems/networks, but while elsewhere — either on the go, at home, or in public spaces such as airports and coffee shops — employees will still need to access sensitive information and data from personal devices that are not as well protected as the corporate-owned systems/networks. The need for employees to responsibly handle data with secure practices, etc., is not a necessarily understood and effective communication.
- **Training IT staff to mitigate risk.** The ongoing development of IT staff skills is important for ensuring that the individuals who are responsible for technology and security infrastructures are up to date on current best practices. Understanding changing technology options and the evolving risk and threat landscape is necessary in order to position the IT team for success. Hence, 79% of respondents said they will improve IT staff training. This is good news on two fronts: 1) ensuring that IT staff are current with their skills and approaches and 2) helping to support retention efforts at a time when demand for talent is high.

- **Revisiting the security strategy.** Organizations are becoming increasingly aware that meeting compliance requirements does not equate to building robust security. Third-party business partners will demand evidence of a strong security and risk management practice as a condition of working together. A forward-looking strategy supports an organization's efforts to build a robust security program as well as to anticipate areas where they need to improve or bring in new skills to address concerns, based on business priorities. Eighty percent of respondents indicated that they were prioritizing the need to develop and execute on a security strategy for IT, devices, and data.

Figure 4

"Which of the following initiatives are likely to be your firm's top IT infrastructure priorities over the next 12 months?"



Base: 887 business and IT decision makers who are involved in decision making for laptops, computers, and other devices
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, September 2019

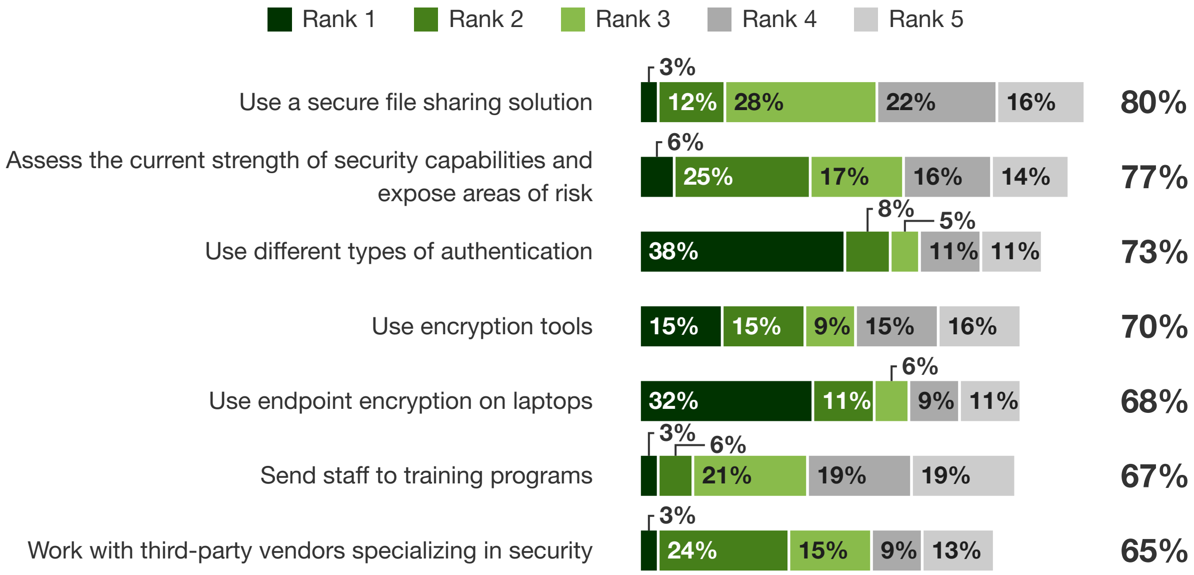
TACTICS TO IMPROVE SECURITY

In the digital age, cyberthreats are everywhere, and breaches make headlines on what seems like a daily basis, costing companies its reputation, capital, and future growth and expansion. In other words, the security of an organization's bottom line depends on the technologies that secure the data, i.e., the fundamental currency of digital business. Data breaches are a unfortunate fact of life. Fifty percent of global network security decision makers said their firm suffered at least one breach in the past year that they are aware of, and that rises to 55% for respondents from enterprises. With this in mind, organizations revealed what elements of security they would like to improve (see Figure 5):

- **Secure file sharing to support employee collaboration.** Technology and employees both play a crucial role in enabling organizations to collaborate and thus create long-lasting economic value. Eighty percent of respondents said they will use a secure file-sharing solution to help improve their security capabilities. However, this should not only be used within the corporate walls of the office, as remote workers and those who travel for work must also be able to access and share files when needed.
- **Authentication to support secure employee access to data.** At its simplest form, authentication solutions keep the bad guys out and the good guys in. With so many data breaches occurring across the globe, the importance of enforcing control is high on the agenda. Seventy-three percent of respondents said they will use different types of authentication, and 38% of respondents ranked authentication as the No. 1 strategic effort they would do to improve security. However, these processes should not hinder employee productivity or get in the way of work getting done; the fluidity of the users' authentication experience makes a big difference.
- **Encryption to control data and meet compliance requirements.** Seventy-three percent of respondents indicated they would employ encryption tools, while 68% specifically pointed to endpoint encryption for employee laptops (full-disk encryption) as what they deemed important for improving security. In a world where it's easy for an employee to lose a device or have it stolen from them, this is a prudent choice. Encryption for data at rest also comes in many flavors, and organizations can choose accordingly based on their needs, i.e., full-disk, file level, media, email, app/field-level, transparent/database encryption.
- **Security assessment to understand current security maturity.** While most security teams have implemented a wide variety of controls and standards to keep their business safe, many are unable to objectively identify where there are security gaps. In turn, they struggle to determine whether they have addressed all the key issues or if some aspect of best practice remains unaddressed. Seventy-seven percent of respondents are aware of this and are looking to improve security by developing precise remediation plans to make sure all components are meeting their desired state of functionality.

Figure 5

"What would you like to do to help improve security?"



Base: 887 business and IT decision makers who are involved in decision making for laptops, computers, and other devices
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, September 2019

Balanced Security Benefits Employees And The Business

Security efforts will enable a business to be more secure, rather than obfuscate its progress with challenges in the pursuit of greater revenue generation. To free the business from barriers, decision makers must take a human-centered and risk-based approach to designing the security experience. As you balance creating a great employee experience with strong security, you can help to (see Figure 6):

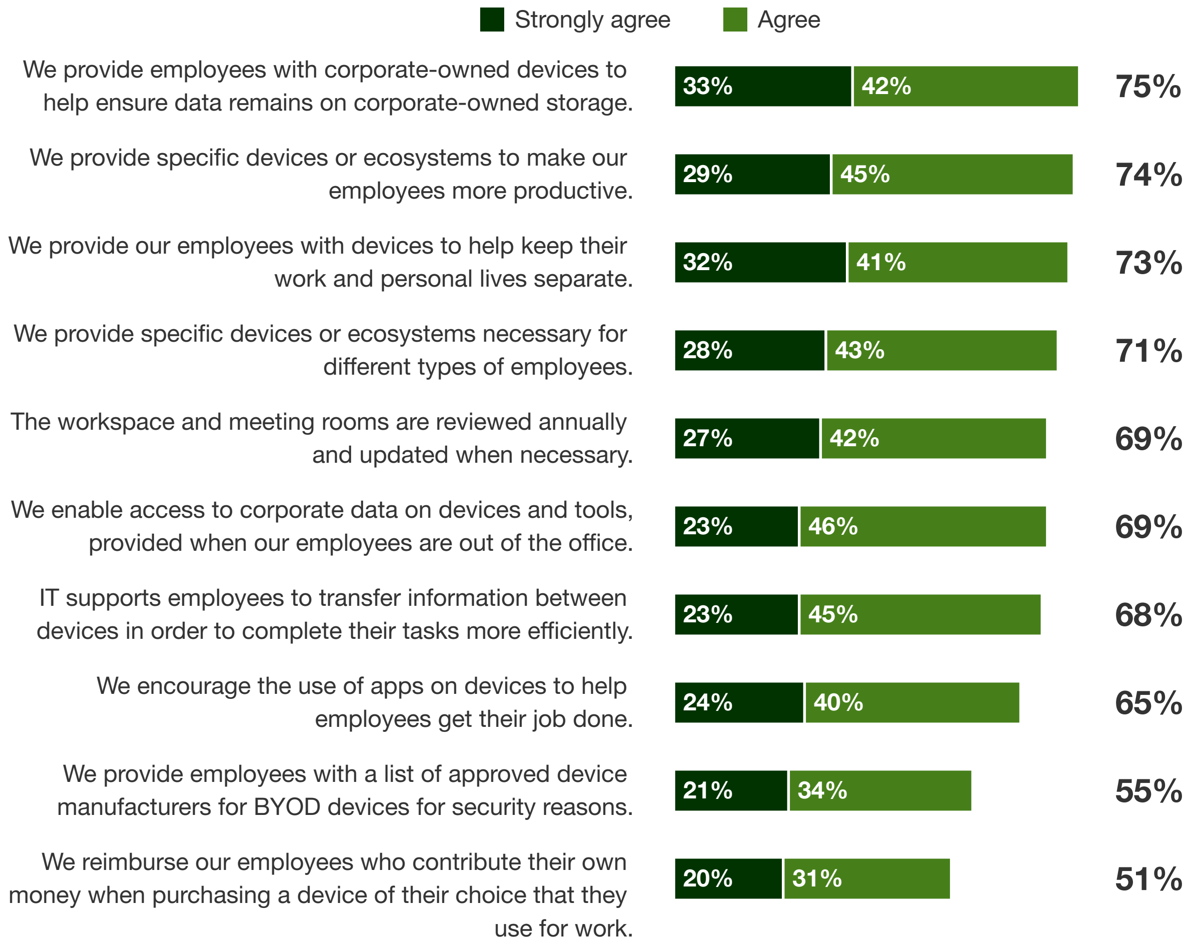
- **Enable remote work to support productivity and competitive advantage.** Whether employees are demanding better support for work-life balance, or your organization is hiring the best person for the job regardless of proximity for commuting into an office, support for remote work is a competitive advantage in hiring and retaining talent. Technology helps to make remote work possible, and security is a critical underpinning for how your firm will securely enable remote work. Sixty-nine percent of respondents indicated that they enable access to corporate data on devices when employees are working outside of the office.

- **Encourage collaboration to spur innovation.** Employees want to share experiences and ultimately, they want to share files and ideas with colleagues. Both the human connection and the tools to help facilitate that connection are prerequisites for curating an environment, or culture, of innovation, especially with a distributed workforce, i.e., employees who are not always face to face with their peers in an office. For now, 49% of respondents say they struggle to enable employees to easily and securely share data. There is room for improvement, in order to realize benefits.

› **Improve the customer experience and reduce employee turnover.** Improving employee happiness through better EX translates to happy customers who receive better support and interactions with your employees. Happy employees are more likely to make the right choices, choices that do right by your customers.[1] One study showed that organizations with happy employees saw an 81% higher customer satisfaction and half the amount of employee turnover.[2]

Figure 6

"What actions has your firm taken to enable remote or flexible work?"



Base: 887 business and IT decision makers who are involved in decision making for laptops, computers, and other devices
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, September 2019

Key Recommendations

Investing in your security infrastructure and controls are a critical component of your security program. However, technology investments alone are insufficient. Determine the right level of balanced security for your organization, based on your specific needs and risk tolerance.

Take four steps today to position your organization for success in achieving the appropriate balance between security and employee experience:

Assess your current state of security maturity. The process of going through the assessment itself may also offer visibility into procedures or processes that are institutional knowledge. As some of these procedures/processes are undocumented, going forward it will be important to unearth the details in case key team members retire or leave the organization. An assessment will provide a view into your organization's existing security controls, processes, and oversight to help determine areas that have potential gaps and need addressing. This assessment will be instrumental in offering guidance for your path forward, in where you need to focus attention and why.

Identify what is sensitive data, why, and where it is located. This includes understanding what data is regulated by compliance requirements, and the value of data for your organization overall. With security controls and appropriate data-handling considerations aside, understanding your data also creates a foundation for supporting the privacy and ethical use of personal data. By having a clearer view and understanding of your data, you are better positioned to determine what is required to protect and appropriately use it.

Understand your organization's level of risk tolerance. While regulations may mandate certain actions and activities, the types of controls and level of control your organization chooses to implement will depend on your level of risk tolerance. Understand the risks to your data and organization and make risk-based decisions for security controls to balance employee needs and productivity.

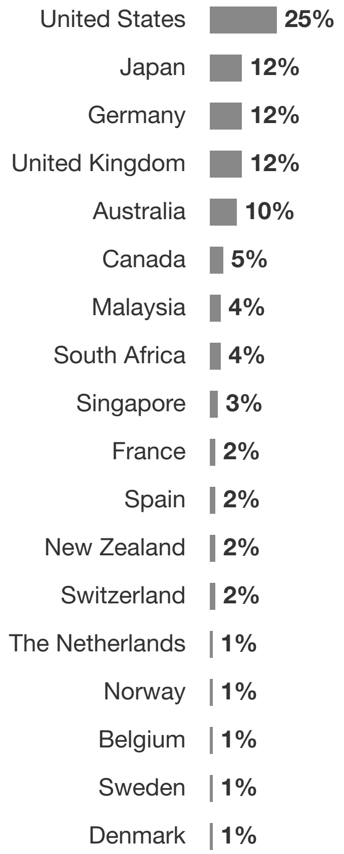
Evaluate how employees work and get their jobs done. Map where security controls influence employees' work experience, and the level of impact it has on their workday and productivity. Different profiles of employees — from the roles that they are in, to the data they have access to in order to do their jobs — will also influence their technology needs, the risks they are likely to face, and the types of security controls you will need to implement to help mitigate those risks. Implement necessary security controls, rather than what will cause unnecessary friction.

Appendix A: Methodology

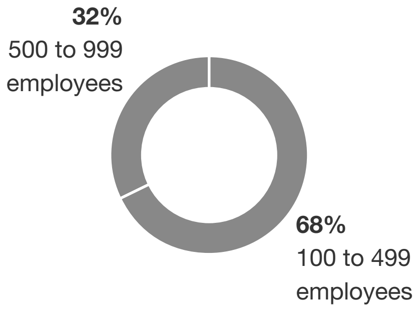
In this study, Forrester conducted an online survey of 887 business and IT leaders across various industries in the market. Questions provided to the participants asked how their spending on security has changed, what influences their security strategy, compliance and regulatory challenges, as well as what the future of security looks like for their organization. The study began in March 2019 and the Thought Leadership Paper was completed in August 2019.

Appendix B: Demographics

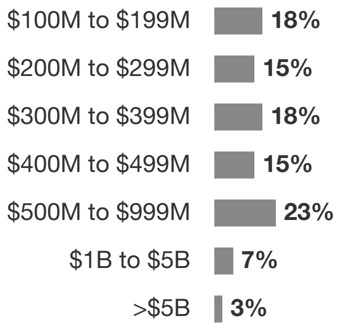
"In which country are you located?"



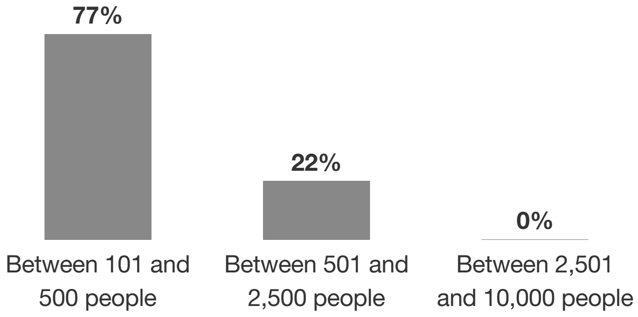
"Using your best estimate, how many employees work for your firm/organization worldwide?"



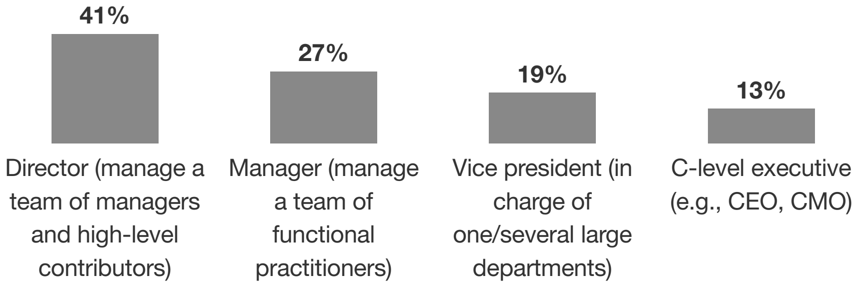
"Using your best estimate, what is your organization's annual revenue (USD)?" (N = 861)



"For the technology and services purchasing decisions that you influence the most, how many employees or members of your organization's workforce do they directly impact?"



"Which title best describes your position at your organization?"



Base: 887 business and IT decision makers who are involved in decision making for laptops, computers, and other devices
Source: A commissioned study conducted by Forrester Consulting on behalf of Dell, March 2019

Appendix C

ENDNOTES

[1] Source: “Transform The Employee Experience To Drive Business Performance,” Forrester Research, Inc., February 12, 2018.

[2] Source: James K. Harter, Frank L. Schmidt, and Theodore L. Hayes, “Business-Unit-Level Relationship Between Employee Satisfaction, Employee Engagement, and Business Outcomes: A Meta-Analysis,” Journal of Applied Psychology, April 2002 (http://www.factorhappiness.at/downloads/quellen/s17_harter.pdf).