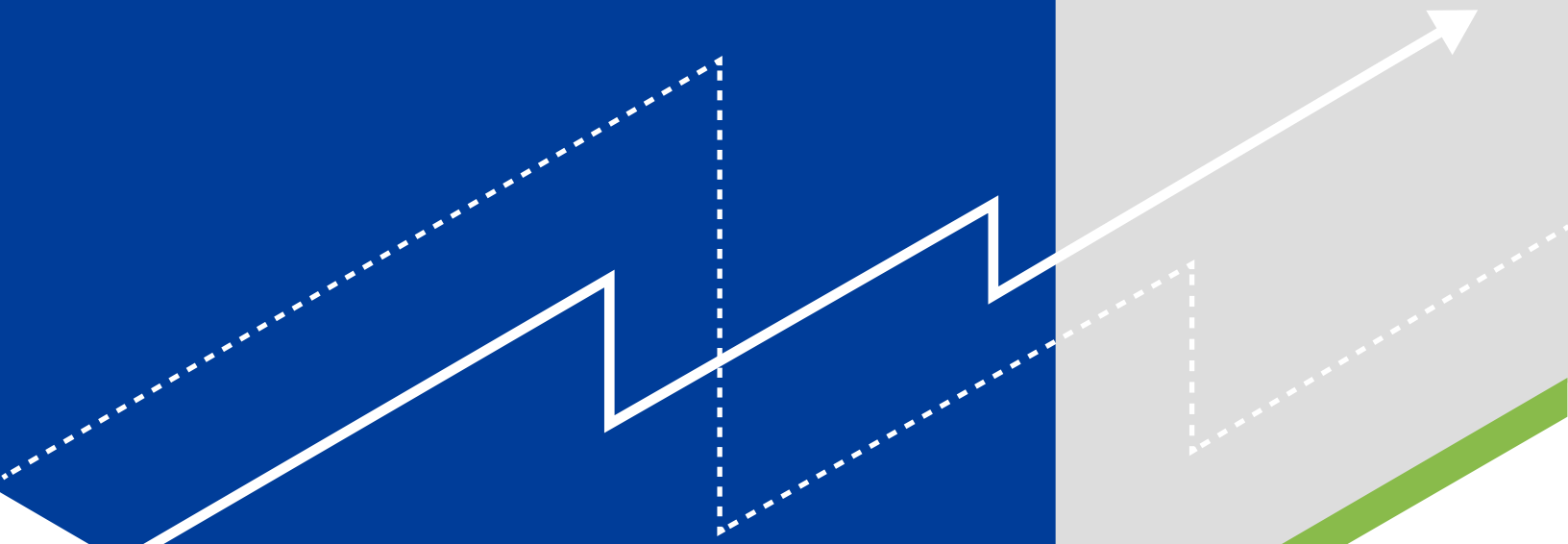
A Forrester Consulting
Thought Leadership Paper
Commissioned By IBM

March 2017

Mobile Vision 2020

The Impact Of Mobility, The Internet Of Things, And Artificial Intelligence On The Future Of Business Transformation



FORRESTER®

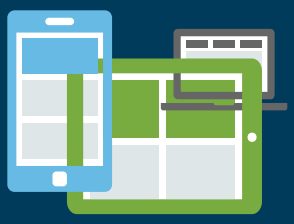
Project Director:
Heather Vallis,
Senior Market Impact Consultant

Contributing Research:
Forrester's Security & Risk 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

As mobile gains more capabilities and access to company data, mobile devices continue to play an important role in how workers do their jobs. Information workers are no longer tied to their PCs — smartphones, tablets, and laptops give them the flexibility to choose the device that best suits the context of each task performed. The internet of things (IoT) represents the next leap in business transformation, changing how enterprises sense, analyze, and control their connected worlds. However, as the number of devices and things that touch sensitive organizational data increases, the complexity of managing and securing a growing attack surface also grows. Employees expect consistency in management and capabilities across all of the devices they use for work; however, the majority of organizations take a disconnected approach, using disparate teams and tools for endpoint management and security. In order to reduce the amount of friction and internal complexity, organizations need to consider both device-specific and device-agnostic approaches dependent on their use cases, where device-agnostic controls are focused at the application and data layers across all device types, regardless of form factor.

Applying artificial intelligence (AI) techniques, such as cognitive computing and machine learning, to the analysis of all the new data created in such a paradigm is not only transformational but required as the device count (and complexity) rises. Organizations will be able to take this flood of data and uncover business insights to further propel the convergence of the management and security of these currently disparate endpoint form factors, leading to a future state of unified endpoint management.

In October 2016, IBM commissioned Forrester Consulting to evaluate the means by which enterprises are managing and securing various endpoint form factors today and how strategies will change over the next three years. In conducting an in-depth survey of 556 IT and security leaders in the US, the UK, Germany, India, and Australia, Forrester found that while enterprises have a decentralized approach to managing and securing smartphones, tablets, laptops, and IoT today, they will move to a more consolidated — and cognitive — approach by 2020.

FORRESTER®

KEY FINDINGS

- **Enterprises have a siloed approach to device and endpoint management.** End user computing is no longer a one-size-fits-all model. Organizations are rapidly shifting from issuing a single PC and image for every employee to an approach that supports multiple devices for workers. IoT is typically managed by lines of business as part of their operations. However, the majority of enterprises still have separate teams and tools to manage all of these devices. The majority of those surveyed (74%) reported that their organizations take a device-specific approach to managing devices and endpoints.
- **Management will become more centralized over the next three years.** As endpoint environments get more and more complex and enterprises place greater scrutiny on device and endpoint management cost of ownership, organizations will begin to move from device-specific to device-agnostic management. By 2020, 42% of organizations will be taking this more centralized approach, up from just 26% today.
- **Many organizations will have unified endpoint management (UEM) in place by 2020.** As organizations work toward a more integrated and device-agnostic approach, implementation of UEM will increase. While just 15% have this centralized management approach in place today, 54% will have deployed UEM solutions by 2020.
- **By 2020, the majority of organizations will leverage AI/cognitive computing to generate insights from endpoint data.** With the expected exponential growth of endpoint data from diverse devices and things, 2020 will see over 80% of companies using AI/cognitive computing to gain business and security insights.

54% of organizations will have UEM solutions in place by 2020.

FORRESTER®

Today's Enterprise Device Environment Is Complex

Today's enterprises are expanding the mobile capabilities they offer to employees. Indeed, the use of mobile devices to perform work-related tasks has become the norm for the majority of workers: According to recent Forrester research, 72% of workers use a mobile device at least weekly for work (see Figure 1).[1] But mobile devices are just one type of tool in today's employee toolbox — roughly half (49%) of information workers use at least three devices for work on a weekly basis.[2] In this modern work environment, it's important that employees are able to select the appropriate device for each task they perform. While smartphones and tablets provide employees the flexibility to quickly access information on the fly or serve customers in real time, laptops and PCs still play a vital role in today's enterprise computing environment. Nearly all information workers (99%) still use a desktop or laptop at least weekly.[3] This proliferation and sophistication of devices present enterprises with considerable management challenges: Approximately one-third (34%) of the IT and security decision makers surveyed cited the increase in the number of supported devices per user among their top five endpoint management challenges.

The proliferation of supported devices per user is a top endpoint management challenge for **34% of organizations**.

Figure 1

The Enterprise Device Landscape: No Longer "One Size Fits All"

72% of workers use a mobile device at least weekly for work

49% of information workers use at least three devices for work on a weekly basis

99% of information workers use a desktop or laptop at least weekly

Base: 7,342 global information workers
Source: Forrester Data Global Business Technographics® Telecommunications And Mobility Workforce Survey, 2016

FORRESTER®

Enterprises Are Managing Devices In Silos

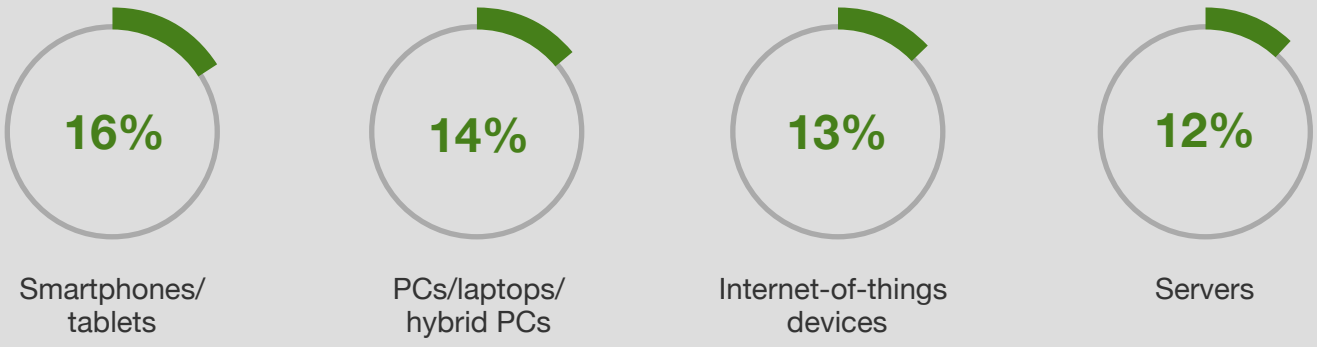
In order to work efficiently and effectively in a diverse device environment, employees need convenience and consistency regardless of the device they are using. Data and tools available on a PC should, ideally, also be accessible via a mobile device. However, the decentralized approach many organizations take to managing and securing devices makes this difficult, if not impossible, to achieve.

ORGANIZATIONS LACK A CENTRALIZED ENDPOINT MANAGEMENT TEAM

Despite the rise in cross-device use, many organizations are still keeping their devices in management silos. Less than one-fifth of the IT and security decision makers surveyed reported having a dedicated team to manage both mobile devices and traditional endpoints. Indeed, most of the enterprises surveyed indicated they had separate groups managing mobile devices (smartphones and tablets); PCs, laptops, and hybrid PCs; servers; and IoT devices (see Figure 2).

Figure 2

"Currently, which group within your organization is primarily responsible for managing the following?"
(Combined mobile/traditional endpoint team)



Base: 556 IT and security professionals involved with client, endpoint, or mobile management and security
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2017

FORRESTER®

ENDPOINTS ARE MANAGED AT THE DEVICE LEVEL

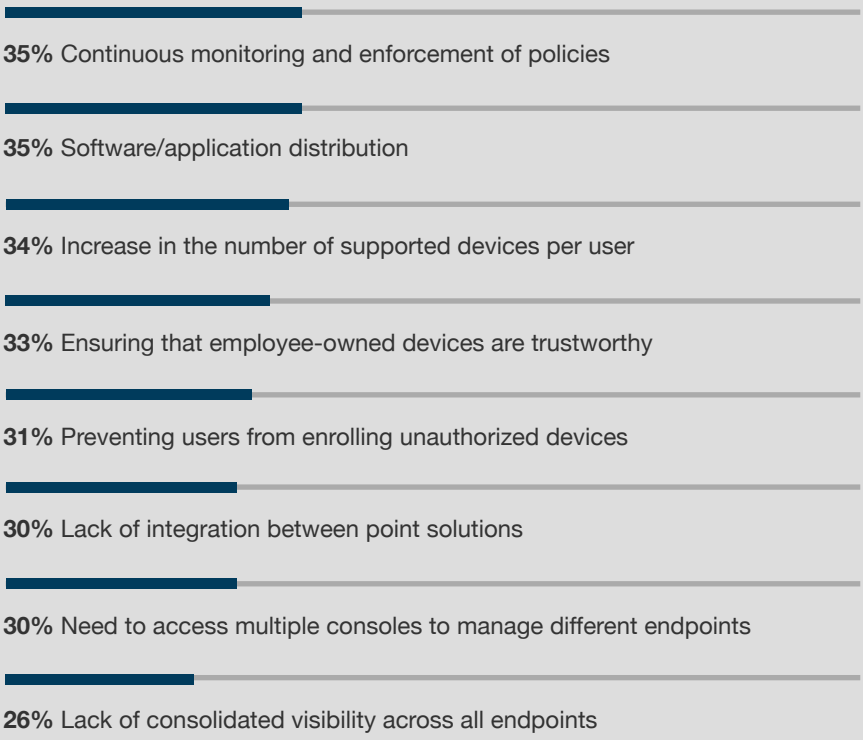
Given this lack of connection between the personnel managing enterprise endpoint form factors, it comes as little surprise that the overarching approach to managing and securing devices is disconnected as well. According to our survey, 74% of organizations are using a device-specific approach, managing device form factors separately. This is likely due in part to the limitations in traditional PC management tools. According to a Forrester survey of telecommunications decision makers, 49% said they invested in enterprise mobile management (EMM) tools because their PC management tools didn't have the capability to manage mobile devices.[4] The result is that most organizations use one solution to manage their PCs and another to manage mobile devices. While this isn't too much of an inconvenience when performing basic management tasks, any patching, software deployment, policy, and configuration could prove to be difficult. Fortunately, PC operating systems are approaching those for mobiles devices in terms of ease of management and security. A disparate approach to endpoint management presents a number of challenges, including:

- **Endpoints are managed via different consoles.** Using different solutions to manage enterprise devices means working in a minimum of two different consoles with different user interfaces (UIs) and functions. Thirty percent of the IT and security decision makers surveyed identified the "need to access multiple consoles to manage different endpoints" as one of their top five endpoint management challenges. These disparate tools also make it difficult to distribute software across complex enterprise environments (35%). Further, in the absence of a single management solution to manage multiple devices, organizations lack consolidated visibility across all endpoints — a problem cited by 26% of respondents (see Figure 3).

74% of organizations are taking a device-specific approach to endpoint management.

Figure 3

"What are your organization's top endpoint management challenges?" (Select up to five)



Base: 556 IT and security professionals involved with client, endpoint, or mobile management and security
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2017

Continuous monitoring and enforcement of policies is the **No. 1 endpoint management challenge**.

› **Each management solution needs to be integrated with other systems separately.** Continuous monitoring and enforcement of policies was the No. 1 endpoint management challenge for survey respondents, cited by 35%. In order to establish consistent monitoring, policies, and controls over all devices, device management solutions need to be integrated with other enterprise solutions, like network access control (NAC) and identity and access management (IAM). Yet 30% of those surveyed reported a lack of integration between point solutions among their top challenges. When devices are managed via different solutions, systems integrations need to occur for each management solution — meaning integrations have to be done multiple times. Duplication of efforts increases the chance mistakes will be made, which can hurt the employee experience and create gaps in security.

FORRESTER®

› **Increasing volumes of endpoint data are collected via disparate tools.** Fifty-six percent of those surveyed indicated the amount of data collected by their organization had increased between 1% and 49% over the past 18 to 24 months, and another 35% reported growth of 50% or more (see Figure 4). And this firehose of data will only increase over the coming years: While 46% anticipate the amount of endpoint data they collect will increase between 1% and 49% over the next three years, 50% are bracing themselves for growth of 50% or more. Organizations can gain significant intelligence from endpoint data, particularly for threat detection and remediation purposes. But the collection of endpoint data via separate tools means organizations lack cross-device visibility, increasing the risk that potential threats aren't addressed in a timely manner. Additionally, fragmented data makes it difficult to gain insights that could potentially inform business and operational improvements.

› **It's difficult to ensure device security.** As the number of devices accessing enterprise data increases, so does an organization's attack surface. According to a recent Forrester study, among information workers using 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.[5] Ensuring the security of these devices is a considerable challenge. Over 30% of respondents we surveyed named "preventing users from enrolling unauthorized devices" and "ensuring that employee-owned devices are trustworthy" among their top challenges.

Figure 4

"How has the amount of endpoint data collected by your organization changed over the past 18 to 24 months? How will it change over the next three years?"

Base: 556 IT and security professionals involved with client, endpoint, or mobile management and security
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2017

FORRESTER®

IoT Adds To Management Complexity

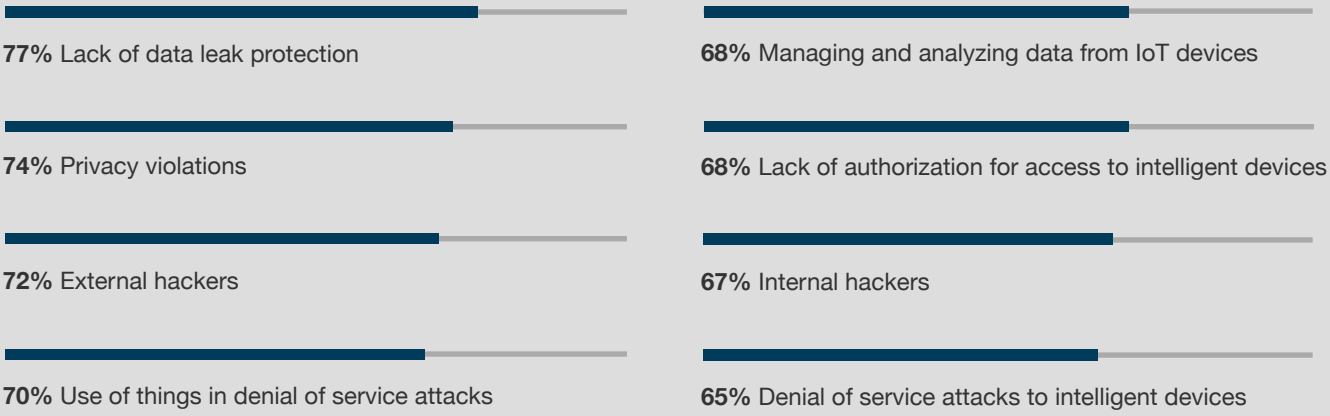
For most organizations, IoT is not a question of "if," but "when." Fifty-seven percent of IT and security pros surveyed indicated their organizations are managing IoT devices now; 88% predict they will be managing these devices by 2020. Yet many (68%) are very or extremely concerned with managing and analyzing data from IoT devices.

Enterprises are adopting IoT devices and applications that will significantly change how they conduct business and serve their customers.[6] But as use of these devices expands in enterprise environments, so do the security risks associated with deploying them. As IoT devices increase in maturity — from dumb objects to fully autonomous, connected devices — the quantity and sensitivity of the data collected, analyzed, and acted upon increases significantly.[7] Top concerns among respondents include a lack of data leak protection (77%), privacy violations (74%), external hackers (72%), and the use of IoT devices in denial of service attacks (70%) (see Figure 5). In order to minimize risk and remain competitive, organizations will need to build out a strategy to manage and secure IoT devices and applications, as well as analyze the vast volume of data collected.

88% of organizations predict they will be managing IoT devices by 2020.

Figure 5

"When thinking about the internet of things (IoT), how concerned is your organization with the following?"
(Percentage very or extremely concerned)



Base: 556 IT and security professionals involved with client, endpoint, or mobile management and security
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2017

FORRESTER®

Mobile Vision 2020

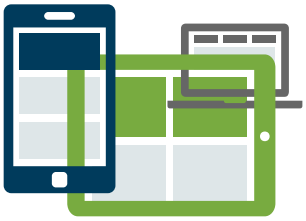
Today's device-centric management approach is not only complex, but costly as well. Separate management tools and teams mean organizations are dedicating considerable resources to tasks and functions that may be redundant and inefficient. As more and more devices come into the organization, employee demands for a more seamless computing experience increase. Wherein the past, users had very distinct and different experiences on mobile versus PC devices, modern PC operating systems are closing — and will continue to close — that experiential gap. With increasing scrutiny on the costs of managing this environment, enterprises will need to evolve their endpoint management strategy.

REDUCING THE TCO OF DEVICE AND ENDPOINT MANAGEMENT WILL BE PARAMOUNT

Enterprises are under the gun to reduce their overall IT spending, be more efficient, and focus on the total cost of ownership (TCO) of their investments. While 73% of respondents reported their organizations are currently prioritizing lowering the TCO of device and endpoint management, the pressure will only increase over the next few years. By 2020, 81% of organizations will be making reducing TCO a high or top priority (see Figure 6). But today's enterprises will need to overcome the challenges of disparate systems, tools, and teams and an overabundance of data in order to meet the mandate to bring down management costs.

CONSOLIDATION WILL PLAY A KEY ROLE IN DRIVING DOWN TCO

Enterprises will need to build a plan to address these device and endpoint management challenges in order to lower TCO, and they must start at the foundational level. Looking ahead to 2020, consolidation of teams and tools will be critical to bringing down the cost of managing mobile devices and other endpoints. The study revealed that organizations anticipate tackling TCO by breaking down departmental silos with a centralized management team (83%) and consolidating their management software to a single platform or vendor (72%) (see Figure 7). Other cost-cutting measures include using a cross-platform license for simplified billing (78%), moving to a subscription model for software (73%), and moving to the cloud with a software-as-a-service (SaaS) or hybrid environment (71%).



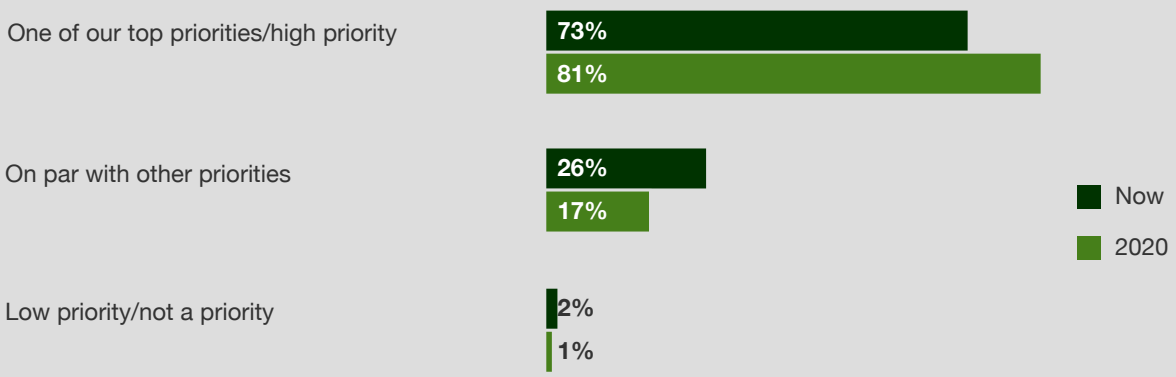
Looking ahead to 2020, **consolidation of teams and tools** will be critical to **bringing down the cost of managing mobile devices and other endpoints.**

Lowering device and endpoint management TCO will be a high or top priority for **81% of enterprises.**

Figure 6

"What priority is your organization currently placing on reducing the total cost of ownership (TCO) of managing devices and endpoints?"

"To what extent do you anticipate reducing the TCO of managing devices and endpoints will be a priority for your organization by the year 2020?"



Base: 548 IT and security professionals involved with client, endpoint, or mobile management and security familiar with their organization's prioritization of device/endpoint management TCO
(percentages may not total 100 because of rounding)
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2017

Figure 7

"Thinking ahead to the year 2020, what is the likelihood your organization will use each of the following methods to reduce the total cost of ownership (TCO) of managing mobile devices and endpoints?"
(Percentage likely or highly likely)

83% Centralized management teams

72% Consolidate management software to one platform or vendor

78% One license used across any platform for simplified billing

72% Hardware/software cost decrease

73% Subscription-based software

71% Decreased enterprise footprint; move to a software-as-a-service (SaaS) or hybrid environment

Base: 556 IT and security professionals involved with client, endpoint, or mobile management and security
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2017

FORRESTER®

ENDPOINT MANAGEMENT WILL BEGIN TO SHIFT TO A DEVICE-AGNOSTIC APPROACH

Device-agnostic controls are focused on the security of the application and data layers across all device types, regardless of form factor. As organizations move toward both organizational and technological consolidation, they will also need to change their approach to managing devices and endpoints. Today, the majority of organizations (74%) take a device-specific approach; however, organizations will start to shift away from this siloed way of managing devices and endpoints over the next three years. By 2020, 42% predict they will be moving to a device-agnostic approach — up from 26% today.

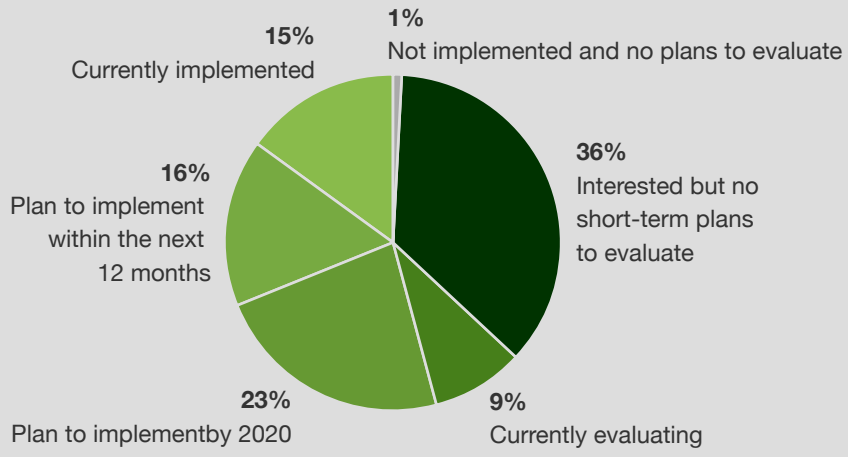
By 2020, 42% of organizations predict they will move to a device-agnostic management approach — up from **26% today.**

UNIFIED ENDPOINT MANAGEMENT WILL PROVIDE THE FOUNDATIONAL LAYER FOR CONSOLIDATION

Unified endpoint management (UEM) is an approach to securing and controlling both traditional endpoints and mobile devices in a connected, cohesive manner from a single console. While few organizations (15%) have adopted UEM today, implementation will increase as organizations work toward a more integrated and device-agnostic management approach. Sixteen percent of organizations will adopt UEM within the next 12 months; by 2020, 54% will have it in place (see Figure 8).

Figure 8

"What are your organization's plans to implement unified endpoint management?"



Base: 556 IT and security professionals involved with client, endpoint, or mobile management and security
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2017

UEM implementation will increase over the next three years as organizations work toward a more integrated and device-agnostic management approach.

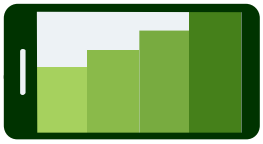
FORRESTER®

UEM adoption will be driven by several factors, including:

› **Device proliferation.** Among those respondents at organizations either using or planning to implement UEM, the primary driver for adoption was an increased need to manage a rapidly growing number of devices, cited by 43%. Fueling this growth is the influx of employee-owned devices: 32% reported that bring-your-own-device (BYOD) policies for smartphones, tablets, laptops, and desktops are an impetus for UEM adoption (see Figure 9).

  One of the main reasons that employees are bringing not only their own mobile devices but also PCs into the office is that today's PCs have evolved, acting more like mobile devices. Modern laptop operating systems are approaching the ease of management and security of mobile OSes. In fact, 40% of respondents cited the increasing adoption of Windows 10 and macOS as a driver for implementing UEM.

› **Centralization of endpoint management.** UEM provides a central point through which organizations have visibility and control across all employee devices. This centralized approach to management means organizations can consolidate both endpoint management teams and tools, thereby reducing redundant tasks and functions and lowering TCO. Approximately one-third of those surveyed are turning to UEM in an effort to centralize teams (37%) and endpoint management tools (33%), while 41% see UEM as a means to lower endpoint management costs.



The **primary driver** for UEM adoption is an **increased need to manage a rapidly growing number of devices.**

Figure 9

"What are the factors that drove — or are driving — your organization to implement UEM?" (Select all that apply)

43% Increased need to manage rapidly growing numbers of devices

41% User demand for access to data anywhere, at any time, and from any device

41% Attempting to decrease total cost of ownership

40% Increasing Windows 10 and macOS adoption

39% Ability to perform analysis and gain insights (cognitive) across all endpoints

37% Simplification of compliance reporting and management

37% Consolidation of teams to manage endpoints

37% Migrating to a software-as-a-service (SaaS) management model

33% Consolidation of endpoint management tools

32% BYOD policy for smartphones, tablets, laptops, and desktops

Base: 304 IT and security professionals involved with client, endpoint, or mobile management and security at companies that plan to implement UEM by 2020
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2017

FORRESTER®

› **Demand for anytime, anywhere data access.** Employees are no longer tethered to their desks; they are performing work-related tasks using multiple devices every day. In order to do their jobs effectively, they need access to the same applications and data, regardless of the device they are using. Roughly two-fifths of the IT and security decision makers surveyed indicated that the decision to implement UEM is being driven by this end user demand for cross-device data access.

› **Need for improved analysis capabilities across all endpoints.** Thirty-nine percent of respondents pointed to the ability to perform analysis and gain insights across all endpoints as a driver for adoption. While it is certainly possible to collect device-specific data through individual device management tools, unless these tools are integrated with other management and intelligence systems, organizations have an incomplete picture. This insight is critical when trying to detect threat campaigns that span multiple endpoint types — such as detecting lateral movement between an employee's corporate smartphone and laptop or any targeted attack against specific users involving multiple endpoint form factors. UEM not only acts as an integration point for other critical enterprise systems but also consolidates endpoint data for more meaningful analysis and actionable insights.

ENTERPRISES WILL LEVERAGE ARTIFICIAL INTELLIGENCE TO MAKE SENSE OF ENDPOINT DATA

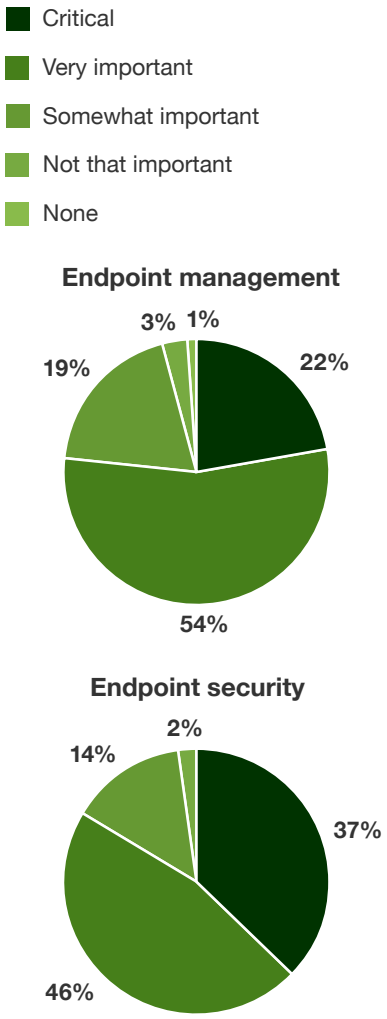
Artificial intelligence (AKA AI or cognitive computing) has been around since the 1950s, but it has become increasingly popular over the past few years due to advances in deep learning and data storage and processing.[8] According to recent Forrester research, investment in AI/cognitive computing will increase by greater than 300% in 2017 compared with 2016.[9] AI/cognitive computing is quickly evolving to automate many manual tasks, improving the ability of businesses to generate actionable business insights, realize operational efficiencies, and identify and remediate threats. AI/cognitive computing is empowering people and systems to work together more collaboratively and efficiently.

Investment in AI/cognitive computing will **increase by 300%** in 2017.

As the volume of data collected from endpoints increases and enterprises work toward consolidating device and endpoint management, AI/cognitive computing will become a necessity. According to survey respondents, over 80% will implement AI/cognitive computing by 2020 to analyze the vast — and increasingly growing — volume of endpoint data they collect. The IT and security pros surveyed recognize the value of applying AI/cognitive computing to their organizations' endpoint data, with the majority indicating it plays a very important or critical role in their endpoint management (76%) and endpoint security (83%) strategies (see Figure 10).

Figure 10

"How important a role does — or will — artificial intelligence/ cognitive computing play in your organization's endpoint management and security strategy?"



Base: 481 IT and security professionals involved with client, endpoint, or mobile management and security at companies that have implemented, plan to implement, or are investigating AI/cognitive computing
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2017

FORRESTER®

Survey respondents identified both security-related and business benefits of leveraging AI/cognitive computing:

- **Applying AI/cognitive to security.** AI/cognitive computing can help organizations make moderate to significant improvements to threat detection and remediation capabilities, including the ability to analyze threats in real time (80%), improve security process efficiencies (79%), recognize patterns in security data that signify threats (78%), and suggest or automate corrective actions (74%) (see Figure 11).

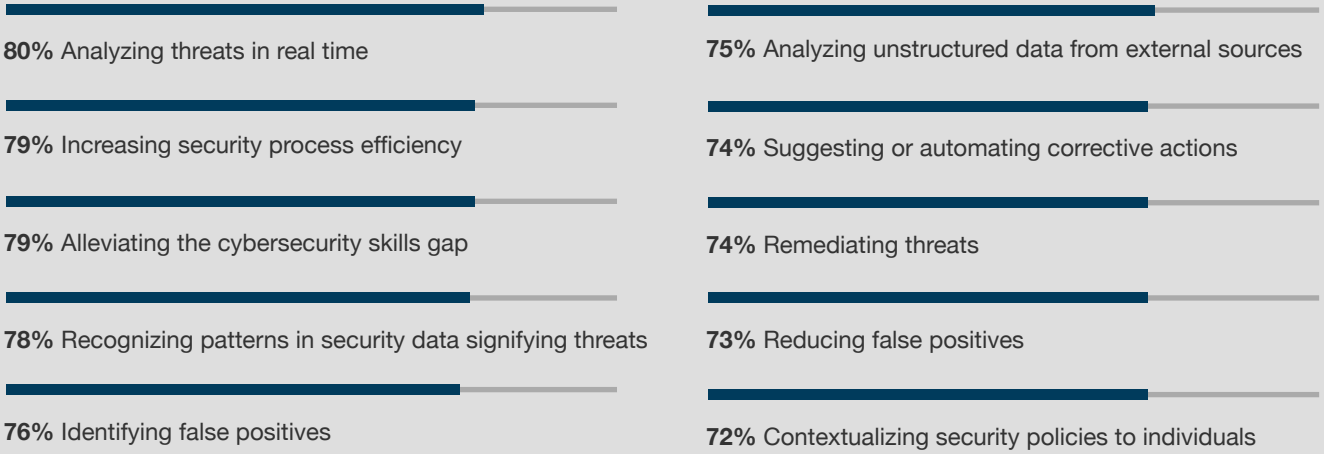
  AI/cognitive computing technologies can efficiently analyze endpoint or structured data, finding patterns and making connections in it much faster than human analysts can and helping to find threats and identify false positives. AI/cognitive can also be leveraged to automate manual security processes — such as correlating threat information, researching threats, and investigating alerts — by allowing analysts to query multiple data sources from unstructured data simultaneously, accelerating the research and investigation process. For example, preventing and detecting modern ransomware requires insight into all executables run on the endpoint as well as in-memory behavior to stop advanced file-less malware variants. Correlating and pulling insights from this data would be incredibly difficult without the use of AI/cognitive computing.

- **Leveraging AI/cognitive for productivity and insight gains.** The majority of those surveyed recognized that AI/cognitive computing can also bolster business efficiencies and productivity. Eighty-one percent said the technology can help make moderate to significant improvements in operations and administration efficiencies (see Figure 12). Beyond this, AI/cognitive can help solve for mobility staffing and skill deficiencies, which were cited by 75% and 71% of respondents, respectively. By automating tasks and functions, device management becomes more efficient, less manual, and more cost effective.

  AI/cognitive computing can provide enterprises with powerful insights through the use of cognitive interfaces in complex systems, advanced analytics, and machine learning technology. This technology can drive faster business decisions by helping close the gap from insights to action. Survey respondents recognize the value in leveraging AI/cognitive computing for this purpose, with over three-quarters indicating the technology would improve their ability to uncover insights from unstructured data in mobility software (77%), analyze IoT data (76%), provide key business insights to benefit the company (76%), and ultimately help them make data-driven decisions (76%).

Figure 11

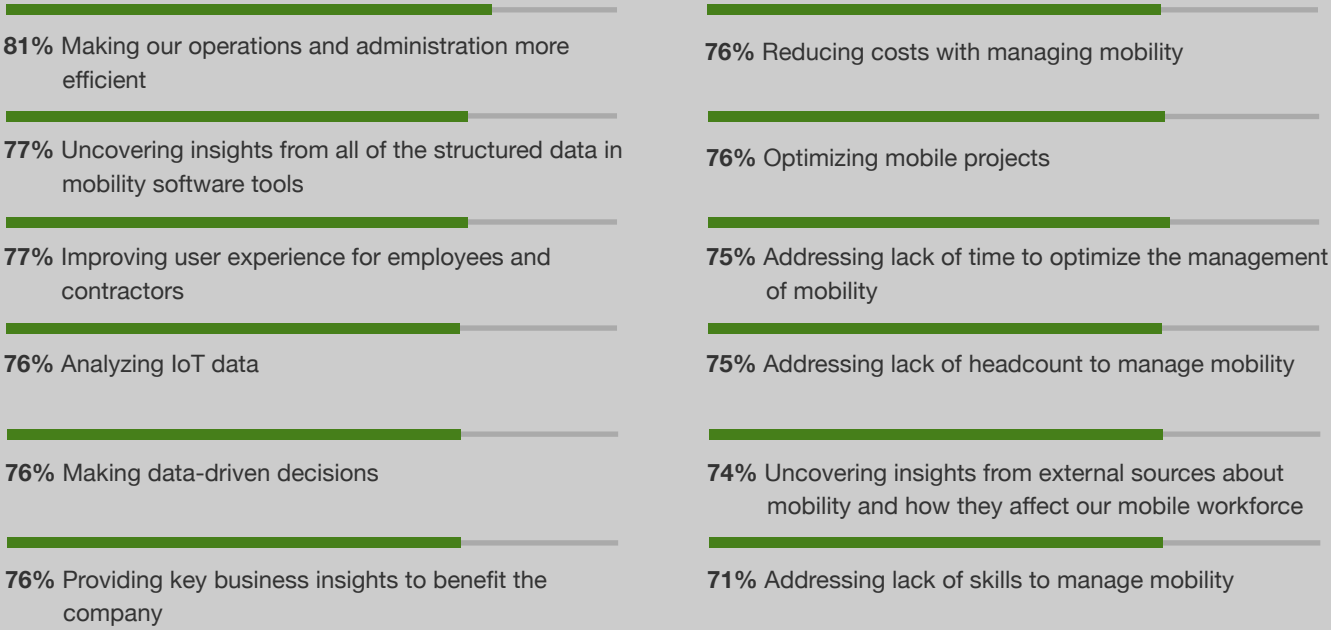
"To what extent has — or could — artificial intelligence/cognitive computing improve(d) your organization's capabilities in the following productivity or business insight areas?"
(Percentage moderate or significant improvement)



Base: 481 IT and security professionals involved with client, endpoint, or mobile management and security at companies that have implemented, plan to implement, or are investigating AI/cognitive computing
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2017

Figure 12

"To what extent has — or could — artificial intelligence/cognitive computing improve(d) your organization's capabilities in the following productivity or business insight areas?"
(Percentage moderate or significant improvement)



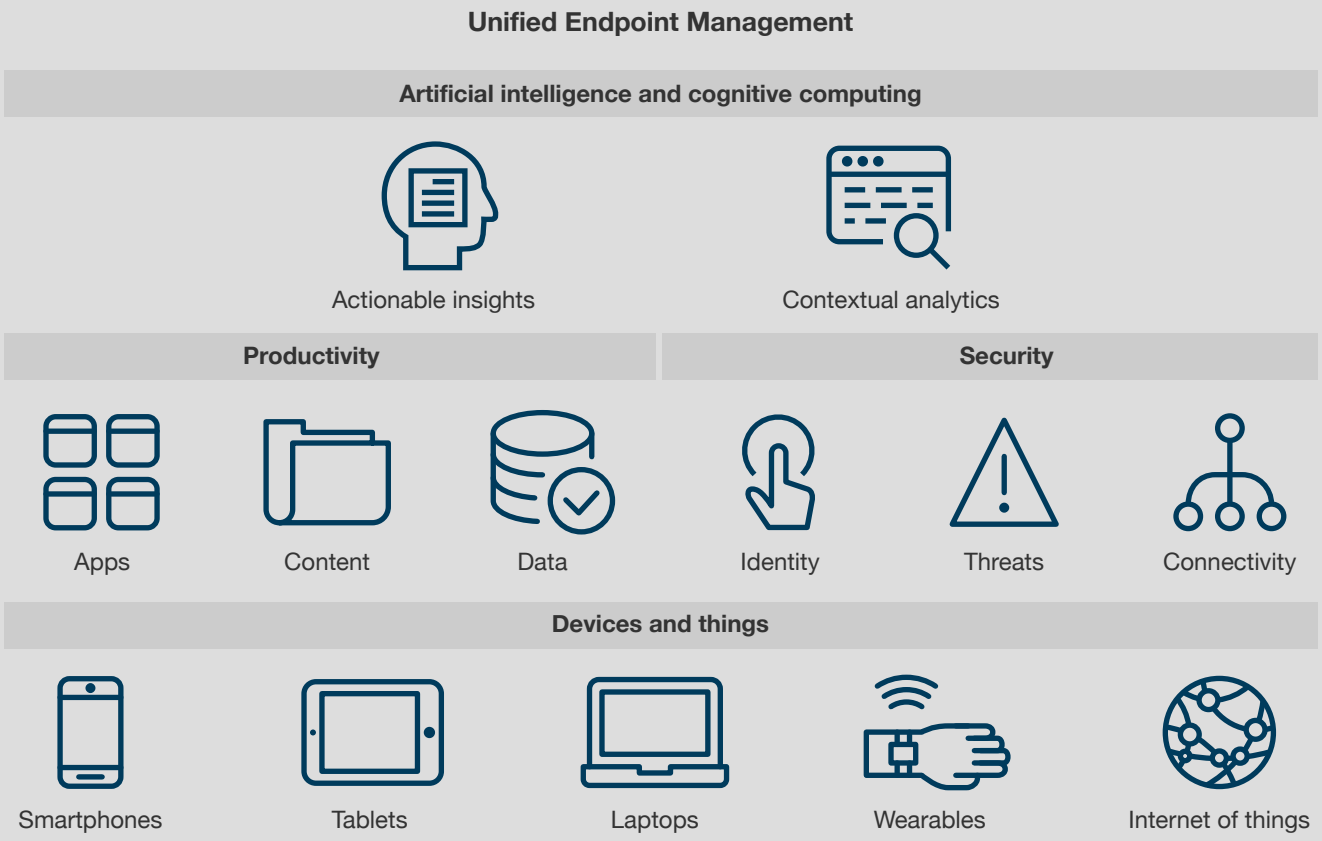
Base: 481 IT and security professionals involved with client, endpoint, or mobile management and security at companies that have implemented, plan to implement, or are investigating AI/cognitive computing
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2017

FORRESTER®

What It Means

Device proliferation will force most organizations to look for ways to simplify the practice of end user device management and security. Today, a majority of organizations treat mobile devices, PCs, and IoT separately, but that will change over the next three to five years as more IT teams adopt tools that allow them to achieve unified endpoint management. Adoption will be accelerated by new advances in computing, such as in the fields of artificial intelligence, cognitive computing, and natural language processing, allowing admins to quickly query their environments and take coordinated action across PC, mobile, and IoT control points. Furthermore, new analysis capabilities will present opportunities for endpoint security and management teams to pull deeper and more meaningful business insights from their increasing amounts of endpoint data while lowering operational friction and TCO.

Figure 13



Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2017

FORRESTER®

Key Recommendations

Begin to shift your endpoint management strategy toward UEM today:

Identify ways to lower your operational friction. UEM presents opportunities in areas such as security operations, management automation, and business intelligence. Look to vendors that integrate with the tools used by your staff, and identify where advanced analytics and automation can help.

Double down on app and data-centric controls. Your UEM strategy will be complemented by strong app- and data-level security and management technologies, such as data containers that protect corporate email, web browsing, and enterprise apps. If you haven't already, begin to shift your focus from device-centric security and management to app- and data-centric strategies. This will allow you to protect what matters — your sensitive apps and data — while raising your device-level risk tolerance.

Understand that IoT will be a huge opportunity for many industries. IT and security leaders need to work with lines of business to understand the opportunities and challenges with IoT and begin talking to UEM vendors about how they can help you manage these endpoints.

Unify your security intelligence and control. Once you have unified endpoint intelligence, advanced analytics and AI/cognitive computing can be applied to gathered data to gain business insights to drive competitive advantage and speed your time to containment when security events arise.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 556 organizations in the US, the UK, Germany, India, and Australia to evaluate the means by which enterprises are managing and securing various endpoint form factors today and how strategies will change over the next three years. Survey participants included IT and security leaders at organizations with 1,000 or more employees. There was an even distribution of respondents from organizations with 1,000 to 9,999 employees and those from organizations with 10,000 or more employees. Respondents were offered a small incentive as a thank you for time spent on the survey. The study was conducted in January 2017.

Appendix B: Supplemental Material

RELATED FORRESTER RESEARCH

"Build A Cross-Functional Mobile Security Team," Forrester Research, Inc., February 22, 2017

"The State Of Enterprise Mobile Security: 2016 To 2017," Forrester Research, Inc., January 12, 2017

"Predictions 2017: Artificial Intelligence Will Drive The Insights Revolution," Forrester Research, Inc., November 2, 2016

"Quick Take: Your Next Security Analyst Could Be A Computer," Forrester Research, Inc., May 10, 2016

"Secure IoT As It Advances Through Maturity Phases," Forrester Research, Inc., January 7, 2016

"The Forrester Wave™: Enterprise Mobile Management, Q4 2015," Forrester Research, Inc., December 4, 2015

Appendix C: Endnotes

RELATED FORRESTER RESEARCH

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

[2] Source: Forrester Data Global Business Technographics Telecommunications And Mobility Workforce Survey, 2016.

[3] Source: Forrester Data Global Business Technographics Telecommunications And Mobility Workforce Survey, 2016.

[4] Source: Forrester Data Global Business Technographics Mobility Survey, 2015.

[5] Source: Forrester Data Global Business Technographics Telecommunications And Mobility Workforce Survey, 2016.

[6] The internet of things (IoT), or what Forrester refers to as the connected world, combines technologies that enable devices, objects, and infrastructure to interact with monitoring, analytics, and control systems over internet-style networks. These IoT-enabled solutions hold vast promise, with the potential to revolutionize customer experience, enhance safety, improve health, and tear away inefficiency.

[7] Source: "Secure IoT As It Advances Through Maturity Phases," Forrester Research, Inc., January 7, 2016.

[8] Forrester defines artificial intelligence (AI) as the theory and capabilities that strive to mimic human intelligence through experience and learning. Today, AI mainly acts as an augmenting intelligence — it enhances the intelligence of humans by providing them with contextual knowledge from data that the human mind alone can't access and process.

[9] Source: "Predictions 2017: Artificial Intelligence Will Drive The Insights Revolution," Forrester Research, Inc., November 2, 2016.