PATHFINDER REPORT

451 Research® | Advisory

Securing the Enterprise of Things

Opportunity for securing IoT with a unified platform emerging as IoT popularity grows

AUGUST 2017

COMMISSIONED BY

BlackBerry®

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

About 451 Research

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

The information contained herein has been obtained from sources believed to be reliable. 451 Research disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although 451 Research may discuss legal issues related to the information technology business, 451 Research does not provide legal advice or services and their research should not be construed or used as such.

451 Research shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

NEW YORK
1411 Broadway
New York NY 10018
+1 212 505 3030

SAN FRANCISCO
140 Geary Street
San Francisco, CA 94108
+1 415 989 1555

LONDON
Paxton House
(Ground floor)
30, Artillery Lane
London, E1 7LS, UK
P +44 (0) 207 426 1050

BOSTON
75-101 Federal Street
5th Floor
Boston, MA 02110
Phone: +1 617.598.7200
Fax: +1 617.357.7495

EXECUTIVE SUMMARY

The Internet of Things (IoT) has the potential to be the next great computing era – overlapping and extending the mobile era and, of course, the PC era, which still clings to relevancy. In 20 years, we will almost certainly reflect wistfully on the days when all of the physical objects and environments we encounter in our day-to-day worlds were not connected to the internet and able to speak with us and each other. The virtualization of the physical world enabled by IoT is already changing how products are made, serviced and monetized. Marginal costs to add connectivity to everyday objects is rapidly approaching zero. While IoT potential is limitless, the challenge to consistently manage and secure ever-growing endpoint estates will test IT's mettle. With IoT endpoints, the volume of data that must be both protected and analyzed will increase exponentially alongside the number of endpoints themselves that must be secured.

Today, a number of factors have conspired to create an unhelpful wall between the security and management of traditional endpoints and emerging IoT endpoints. Some challenges are related to legacy investments in vertically integrated security and management systems that support only one class of endpoints. Another challenge relates to how organizations manage responsibilities – for instance, IT often manages traditional endpoint environments while operational technology (OT) or line-of-business (LOB) managers have responsibility to manage IoT initiatives, including securing IoT endpoints. This is despite a long list of common requirements and cost-saving potential. Our survey of 200 IT decision-makers directly or indirectly responsible for endpoint decisions in their organizations revealed that they desire and would embrace a better option. The appeal of unifying ***all*** enterprise endpoint security and management within a single system is strong, but some challenges still remain.

Key Findings

- 63% of survey respondents believe that security concerns around digital technologies and processes are the biggest inhibitors to digital transformation.
- 78% of survey respondents said they would be interested if there were solutions available to manage all enterprise endpoints (legacy + IoT). Another 15% of respondents said they might consider one solution to manage all enterprise endpoints.
- 35% of respondents from very large organizations (with more than 10,000 employees) indicated that they see no barriers to investigating unified endpoint management solutions, while 28% of midsized organizations (999-9,999 employees) indicated the same.
- 39% of respondents from very large organizations revealed that a lack of collaboration among internal departments is a potential barrier to unified endpoint management. 51% of midsized organizations believe this is a barrier. Leaders must take action to ensure that IT is prepared to support the wider digital transformation goals of the organization.
- IT is the department most likely to lead oversight of a joined mobility and IoT strategy; 7 out of 10 respondents report that IT is responsible for defining their organization's mobility and IoT strategy.
- IT is also largely responsible for key aspects in the deployment of IoT. Nearly 50% of respondents reported that IT is responsible for endpoint security, management and governance, and device security.
- IT and LOB are both responsible for endpoint security budgets. Nearly 40% of respondents report that LOB or IT are responsible for endpoint security budgets.

Methodology

We surveyed 200 enterprise IT decision-makers in June and July 2017. We received responses from C-level and director-level positions, including CTO, CIO, director of IT, IT Ops or DevOps, VP, and manager of IT. All of our survey respondents had direct influence or decision-making authority on endpoint spending decisions at their firms. Respondents were from the US, UK, Australia, Canada, France, Netherlands, Singapore, Norway, China and Austria.

Our respondents represented a fairly even split of healthcare, financial services, transportation and government organizations. About half were with organizations of 249-1,000 employees and half with 1,000+, including 12% with more than 10,000 employees. This vertical focus was built in by design given complex endpoint environment driven in part by adoption of IoT solutions.

In terms of attitude toward new technology adoption, there was a fairly even split between first adopters, early majority and late majority adopters. Only 4% of respondents identified their companies as laggard adopters of new technology.

Introduction

It's difficult to overstate the enormity of changes that have occurred across the IT landscape over the past decade, yet they pale in comparison to what lies ahead. The stunning positive impact of the invention and mass proliferation of smartphones and tablets also drove a chaotic period that required IT management to rapidly transform itself to manage the new normal of BYOD-driven endpoint security and management, as well as cloud services. And just as we started to believe that the endpoint challenge was somewhat firmly in hand, along came the Internet of Things, bringing a whole raft of new security and management challenges to IT's doorstep.

Today, enterprise mobility and IoT are most likely to be managed and secured in discrete 'silos,' but we predict they will be integrated through IT and managed holistically. The respondents to our survey agree and are seeking solutions that can fulfill that promise. This points to the growing realization that businesses will need to modernize their internal and external application environments to support an increasingly fragmented world of endpoints in which a growing majority of business is conducted by people using mobile computing devices such as smartphones and tablets, and enterprise endpoints explode, driven by the operational advantages of IoT.

In this Black & White paper, we present the results and analysis of a survey of enterprise IT decision-makers to get a sense of the current drivers, challenges and organizational dynamics of the market for endpoint management and security solutions.

Enterprise IT and IoT

Businesses have long relied on enterprise IT leaders to deliver the appropriate infrastructure to support the increased diversity of endpoints employees want to use. Most IT leaders aim to offer flexibility to their users while protecting company data and employee identity, all while securing their infrastructure – all of this takes place against a backdrop of advanced cybersecurity threats and a complex and dynamic regulatory landscape in many vertical industries. With IoT, the nature of IT's relationship with LOB and OT stakeholders will change; IT will be called upon not only to support employees but also fundamentally support digital transformation initiatives at the center of the business.

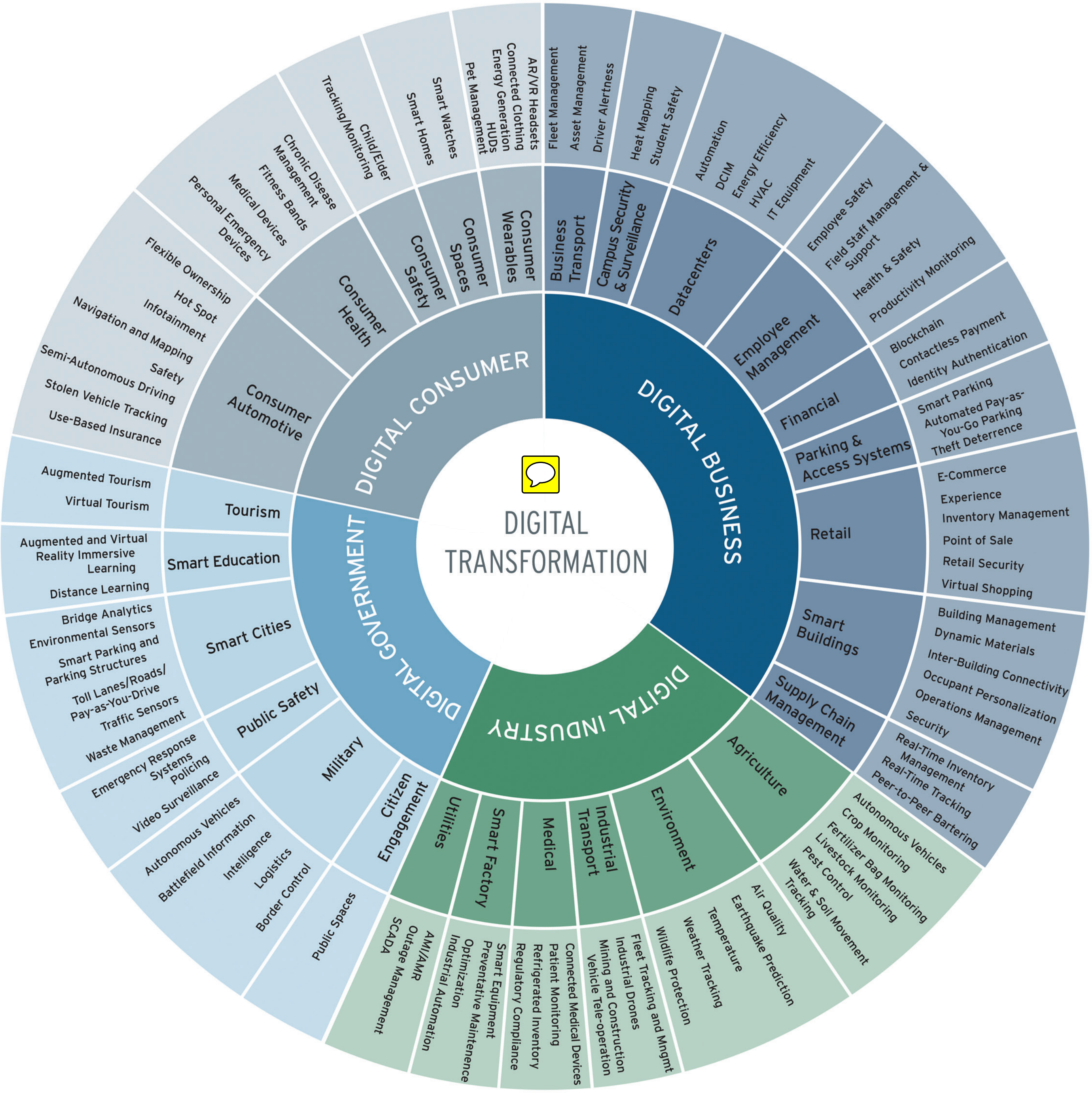
In short order, the support IT offers to employees and partners will extend to machines and sensors. IoT has become shorthand for the rollup of all discrete market activities involving the virtualization of the physical world. The Internet of Things came out of the days of embedded computing systems, machine-to-machine communications, and supervisory and control systems. These technologies allowed for the collection and analysis of machine-generated data and/or the ability to remotely control industrial infrastructure such as energy meters and factory equipment.

451 Research breaks the IoT market down into four classes of product subcategories: consumer, enterprise, government and vertical-specific uses. (See Figure 1.) The enterprise segment of the IoT market is perhaps the most interesting and nascent of all of the submarkets because it anticipates the evolution of IoT from its vertically integrated (siloed) and proprietary OT beginnings to a standardized and integrated future with the full support of enterprise IT tools, platforms, processes and organizational alignment. Some vendors have taken to branding this important submarket as 'The Enterprise of Things.'

We believe this level of integration best represents the true vision for IoT. Such systems will enable seamless interaction and data exchange with IoT subsystems in the enterprise setting – the worker environment, supply chain, physical infrastructure, datacenters, etc. Enterprise IoT systems could benefit from unified management and security platforms. Our survey assessed enterprise demand and readiness.

Figure 1: IoT market taxonomy

Source: 451 Research, 2017



Digital Transformation: Security and Skills Top Concerns

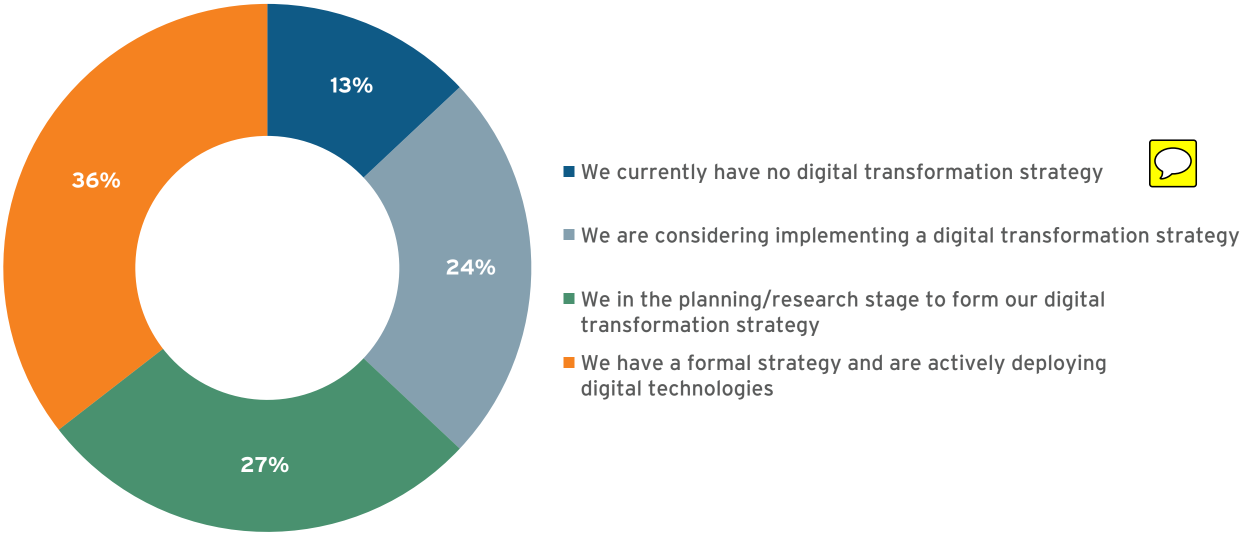
Business leaders face unprecedented opportunities to create stakeholder value through the digitization of business operations. Digital transformation encompasses the fundamental changes enterprise leaders make in terms of technology, people, partners and processes to unlock the potential of the latest innovations in IT technologies and service delivery and human skills. Key enabling technologies underpinning digital transformation include private and public cloud, mobility, social business, big data/analytics and IoT.

Many enterprises operating in the developed world have embarked on their 'digital journey,' but the majority are still at the beginning or planning stages of this journey, or in the 'silo' phase – meaning that they may deeply or widely experiment and iterate with digital initiatives but keep broader enterprise exposure contained to a specific project, region or line of business, namely forgoing the complexity and risk of integration into existing IT processes and systems. (See Figure 2.) How would you rate your own organization?

Figure 2: Charting the digital transformation journey

Source: 451 Research, 2017

Which of the following best describes your organization's status with regard to digital transformation?



Given the impact of digital transformation on the enterprise – both positive and negative – the C suite must actively plan how to best organize the enterprise to unlock the potential of digital transformation. Executives must evolve business processes, ecosystems and internal skills to translate digital capabilities to meet core business goals (make money/save money/save time) in the context of complex environments of legacy investments and processes. Those at the beginning or planning stages of this journey have the advantage of time. By that we mean the opportunity to make more intelligent technology decisions than early movers who had less experience and fewer choices of suppliers in areas such as cloud, data analytics and unified endpoint management.

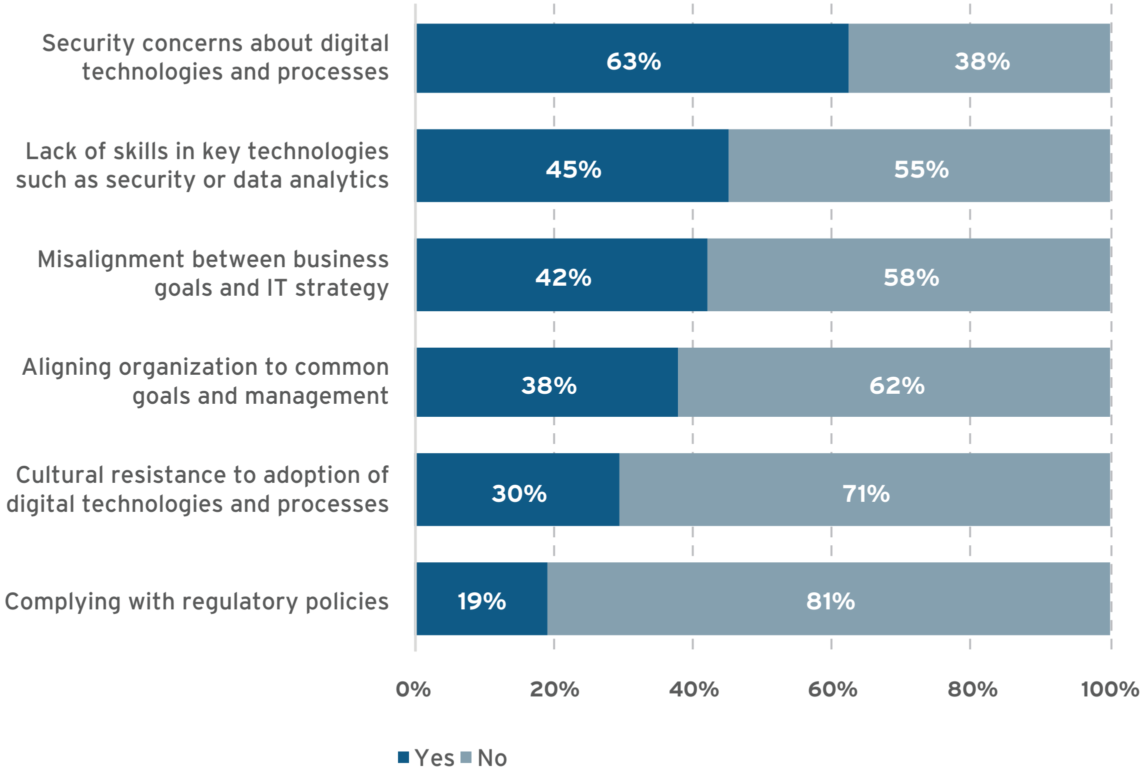
In our survey, we asked about goals related to digital transformation. We received a variety of answers, but by far, the leading response from our survey was 'increase operational efficiency,' with 31% of respondents choosing it as the primary goal. Coming in second was 'lower IT costs,' with 16% of respondents, far ahead of choices such as compliance, which was 7%.

Although IT leaders are at different stages of digital transformation, we asked about what risks their organizations face that could negatively impact their digital transformation initiatives. Perhaps not surprisingly, the leading inhibitor was 'security concerns about digital technologies and processes' with 63% of respondents citing it as the biggest obstacle, while 'lack of skills in key technologies such as security or data analytics' received 45% of the total, and 42% cited 'misalignment between business goals and IT strategy.' This 'snapshot in time' survey is apt in that it reminds us that security is job one in the digital context, and deploying solutions that remove complexity and that can be easily aligned with business goals should be favored.

Although they were not cited as the biggest barriers facing digital transformation, the cultural challenges associated with digital transformation still resonated with respondents. This challenge is particularly relevant in the context of the growing need to converge the skills, processes, technologies and organizational elements of OT and IT. While much of the maturity in the IoT market has occurred on the OT/LOB side of the enterprise organizational chart, systems will require the full support and participation of IT to exploit all of the possibilities that come with integrating data assets, the more prevalent use of standards and open source technologies, and security – the in-depth approach to securing enterprise data at rest and on the move while physically securing the vast array of enterprise endpoints.

Figure 3: Obstacles to digital transformation

Source: 451 Research, 2017
Which of the following are obstacles to successfully achieving digital transformation goals?



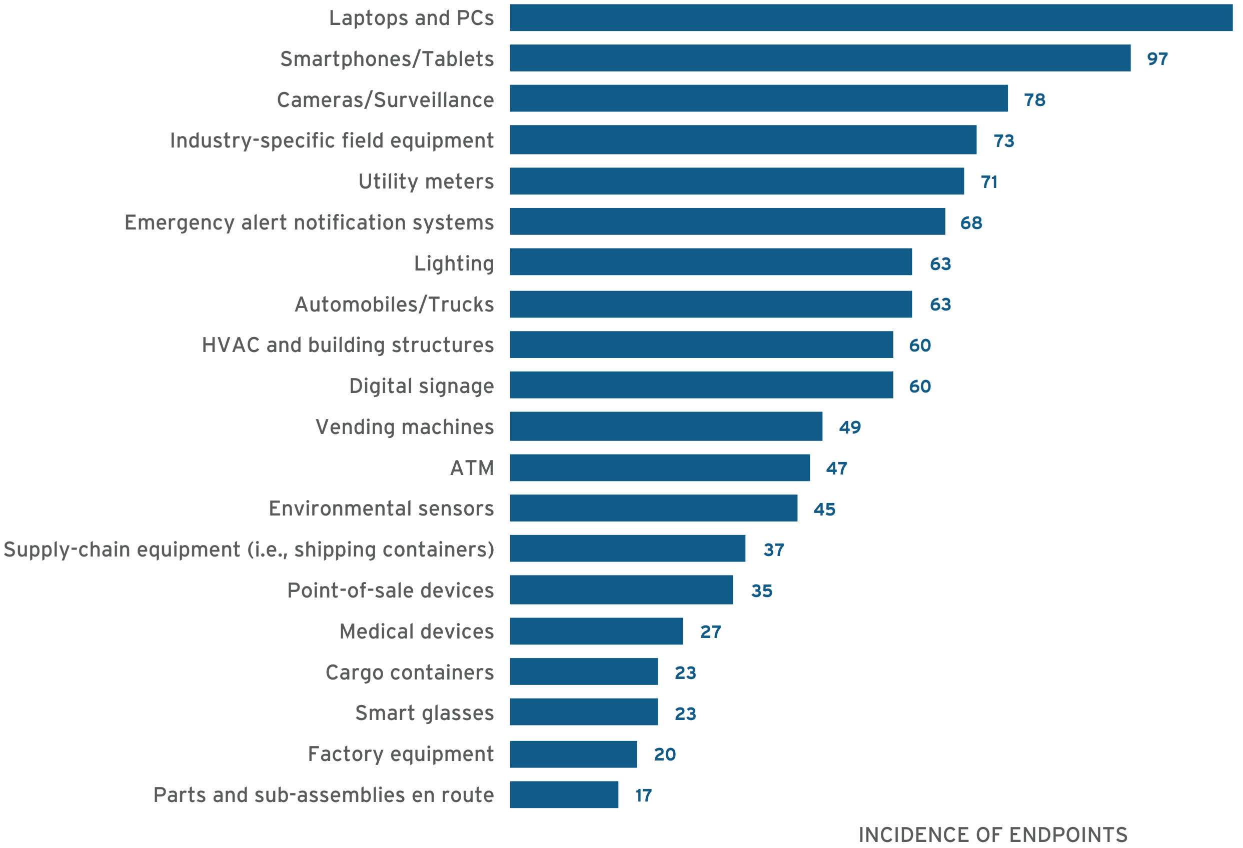
Enterprise Endpoint Explosion: A Very Long Tail

In our survey, we asked respondents to identify their endpoints under management, and we received the familiar long tail of responses. We offered a write-in option, and many respondents came back with common IT endpoints such as laptops, servers, PCs and mobile computing devices to go with a broad list of connected endpoints such as temperature sensors, freezers, ambulances, barcode readers, IT equipment, vehicles, trucks, wearable trackers and emergency response trackers, cargo containers, shipping containers, and pre-production parts and sub-assemblies that are tracked through work-in-progress flows. This growing and diversified list of connected assets is providing valuable data for business leaders to manage their operations more efficiently, create new business models, reduce enterprise risk, or create new ways to engage customers.

Figure 4: Endpoints in use – the long tail (multiple responses allowed)

Source: 451 Research, 2017

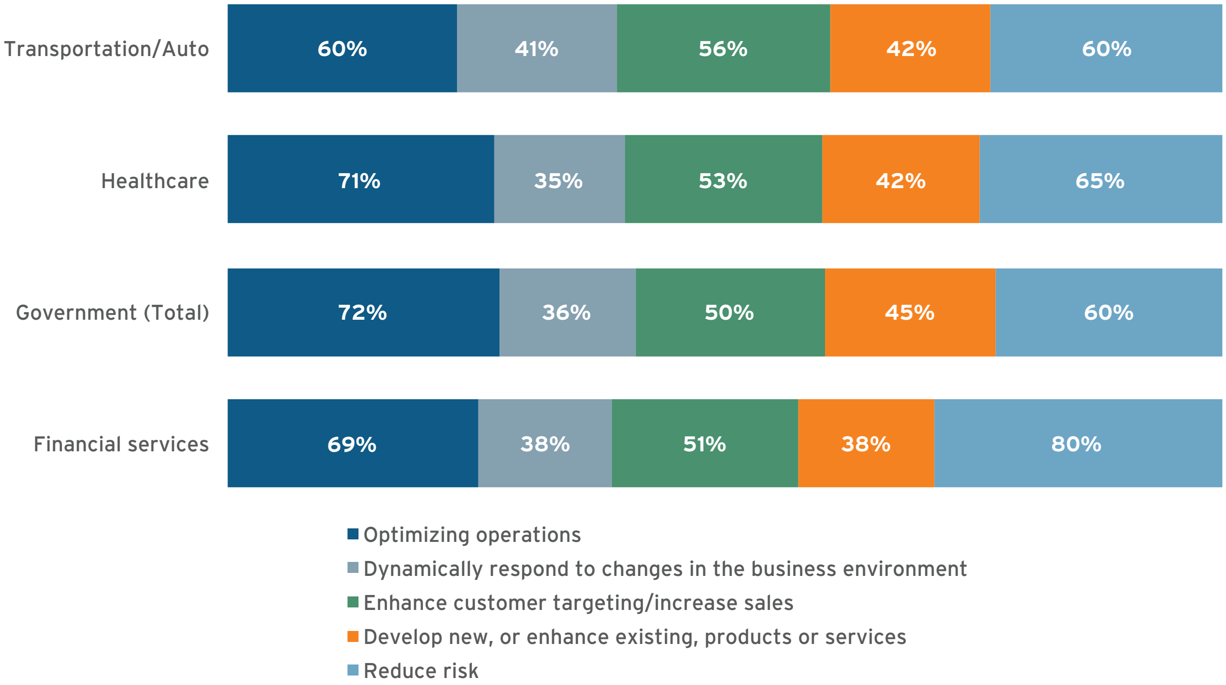
Does your organization collect data from the following endpoints?



In Figure 5, we note that data generated by a diverse set of endpoints is being used to optimize operations and enhance customer targeting to enhance sales. In this cut, we have cross-tabbed industry verticals by the incidence of 'yes' responses to the following options: optimizing operations, enhancing customer targeting/increasing sales, reducing risk, dynamically responding to changes in the business environment, and developing new, or ehancing existing products and services. It makes sense, for instance, that 80% of all financial service respondents indicated that endpoint data is being used to reduce corporate risk.

Figure 5: Endpoint data usage

Source: 451 Research, 2017
Does your organization use data collected from endpoints for any of the following reasons? N=200.



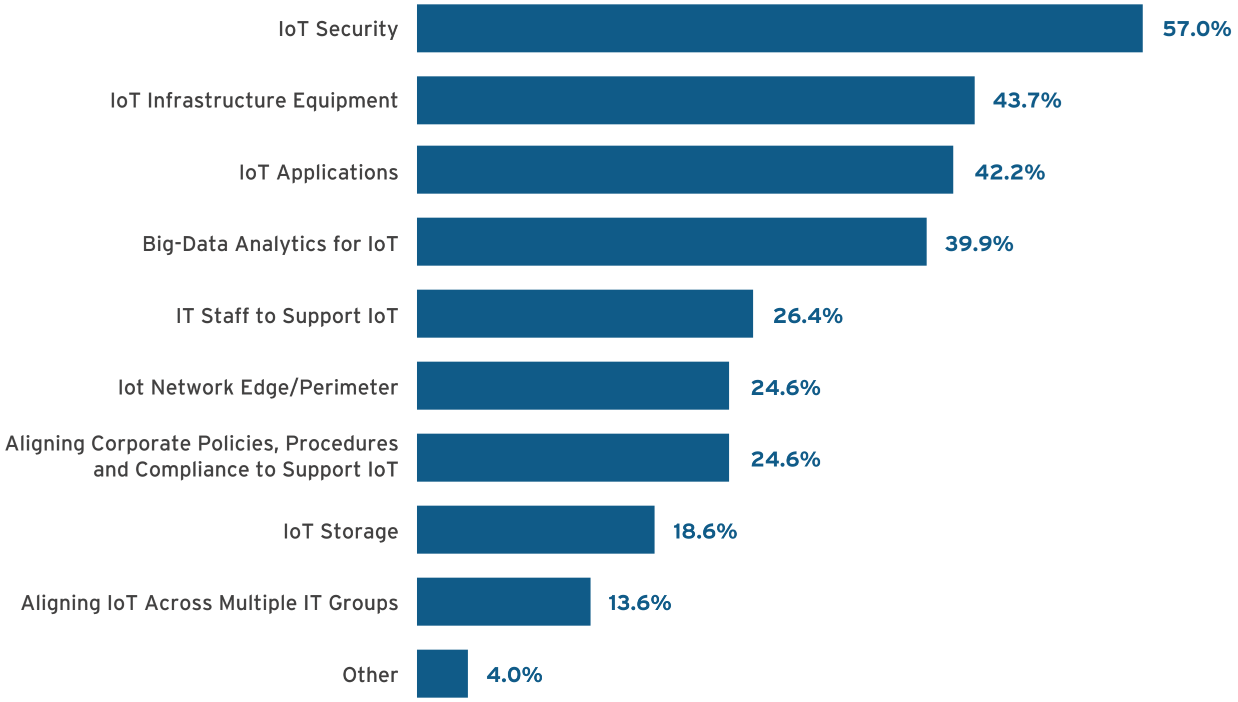
Endpoint Security and Management: Today and Tomorrow

As with all other areas of IT, security and governance are vital considerations when it comes to enterprise digital transformation. Ensuring that users of IoT systems and smart devices remain safe and secure – which requires that their data stays protected and carefully governed – is essential if businesses are to initiate successful IoT projects. As we have tracked over several quarters of survey work with the Voice of the Enterprise: IoT, security remains the top challenge and, therefore, the highest-priority technology for deployment in support of IoT initiatives. (See Figure 6.)

Figure 6: High-priority technologies and processes for IoT in 2017

Source: 451 Research, Voice of the Enterprise: Internet of Things, Workloads and Key Projects 2017

Which of the following technologies or processes are high priorities for your organization to deploy in 2017 for your IoT initiatives? Please select all that apply. N=398.



IoT Requirements

The sheer scale and public nature of the Internet of Things poses a variety of technical challenges for IT planners. Network and system architects must upgrade IT infrastructure to address the increased scalability, reliability and security demands of IoT.

- **Scalability.** The Internet of Things introduces unprecedented scalability considerations because of the vast number of devices generating massive amounts of data. An individual intelligent system might gather and analyze billions of data objects from millions of distinct endpoints, presenting unparalleled data collection, processing, storage and networking challenges.
- **Reliability.** IoT-based applications and automated business processes impose stringent system availability demands. Many intelligent systems will be employed for mission-critical applications where system downtime can result in diminished productivity, dissatisfied customers or lost revenue. Some intelligent systems – emergency services, medical applications and surveillance solutions – will be used in safety-critical applications where system downtime can lead to loss of life or property or cause significant environmental or health hazards.
- **Security.** The distributed nature of IoT implemenations presents a myriad of security challenges. Intelligent systems may rely on the internet for connectivity or use cloud-based compute or storage resources. Security systems and practices must be extended to protect against data loss, service theft and increasingly sophisticated denial-of-service attacks in a scalable manner. Intelligent systems must support cohesive authentication, authorization and auditing capabilities to establish trust, govern access to resources, and ensure compliance with governmental regulations and corporate policies. And they must support strong encryption schemes to safeguard data confidentiality and protect intellectual property.

The pursuit of enterprise endpoint security will necessarily require a massive transformation with the increasing popularity of IoT. While the BYOD challenges of personal smart device usage for getting work done continues to be a strong focus for IT leaders, the challenge is now constantly expanding, like the universe itself.

We asked our respondents how they secure and manage their current IoT deployments. The most popular answer was multi-purpose IoT platforms from 39% of the respondents. Second most popular (with 32% of responses) was device-specific platforms – i.e., for management of security cameras, which was cited by 39% of respondents. The third most popular option for managing non-traditional endpoints was PaaS options from cloud providers such as AWS and Microsoft Azure (with 16.5%), and finally, 10% cited offerings from telecom operators such as AT&T, Verizon, Vodafone, etc.

The Case for Unified Endpoint Management

The time has come to look at traditional and mobile endpoints and IoT endpoints for what they really are: foundational elements of digital transformation. When you step away from self-inflicted organizational and technology silos, it becomes clear that these are digital initiatives that share a common set of business objectives, underlying technology requirements and challenges.

COMMON ENDPOINT REQUIREMENTS

- **Scalability.** Both IoT and traditional endpoint management introduce unprecedented scalability requirements, with vast numbers of devices and objects generating massive amounts of data. An individual system might gather and analyze billions of data objects from millions of distinct endpoints presenting unparalleled data collection, processing, storage and networking challenges.
- **Diversity and growing endpoint support.** A common framework for IoT and traditional endpoint management will require support for an increasingly diverse set of endpoint capabilities. Adding IoT to the mix introduces significant fragmentation because the choice of operating systems is reflective of the level of overall market fragmentation, mixture of vendor-driven and open source alternatives.
- **Reliability.** IoT and traditional enterprise endpoint-based applications and business processes impose higher system-availability demands. Some of these systems will be employed for mission-critical applications where system downtime can result in diminished productivity, dissatisfied customers and lost revenue. Others will be deployed in safety-critical applications – in emergency services, medical applications and surveillance solutions, for example – where system downtime could lead to loss of life or property or cause significant environmental or health hazards.
- **Security.** Both IoT and traditional enterprise endpoints present a myriad of security challenges. In both cases, these systems often rely on the open internet for connectivity or use cloud-based compute or storage resources. Security systems and practices must be extended to protect against data loss, service theft and, increasingly, sophisticated denial-of-service attacks in a scalable manner.
- **Reporting and analytics.** IoT and traditional enterprise endpoints need to provide up-to-the-minute information on app, device and user activity to gain insights into user, network and device behavior.
- **APIs and microservices.** Both IoT and traditional enterprise applications need easy replicability in the technical method and documentation around the integration of applications into back-end data sources. The monitoring and maintenance of application service APIs should be created and managed centrally in the platform and provide reports on usage and performance, as well as built-in troubleshooting tools.
- **Support developers:** Different stacks, protocols and standards weaken developer productivity by elongating the lifecycle and making the automation of application and infrastructure delivery more complicated. Strong developer tools support innovation by reducing the number of channels and cumbersome processes needed to create and launch applications.
- **Deliver consistent user experience**. Consistent user experience for enterprise mobility and IoT applications is a critical success factor for any digital initiative that involves a user interface. Getting the user interface right is complicated in part by mobile-specific considerations associated with small screens (or no screens for IoT), variations in device features, constraints in usage and connectivity, and usage context.

SURVEY SHOWS STRONG INTEREST IN UNIFIED APPROACH TO ENDPOINTS

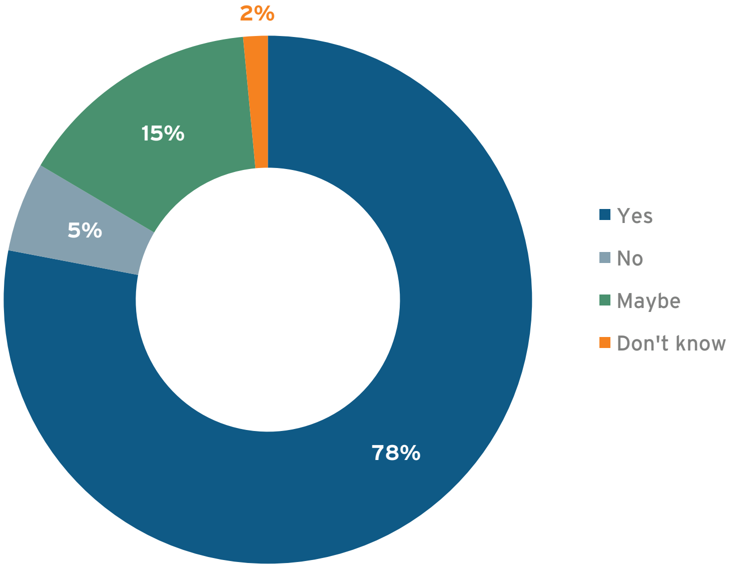
Within our survey, we asked a number of questions regarding the concepts of unified endpoint security and management. The first question was 'How important do you view the ability to have consistent management and security across all endpoints?' **Seventy-six percent of respondents replied 'Very Important' while another 22% replied 'Somewhat Important.'** Given the overwhelming view that management consistency across all endpoints is important, we next asked about interest in acquiring such a solution.

When we asked our survey respondents whether they would be interested in a solution that would allow them to manage all of their endpoints in one place, the results were overwhelming in the positive with nearly 80% saying 'Yes' and a further 15% saying 'Maybe.' (See Figure 7.)

Figure 7: Interest is high for unified endpoint management

Source: 451 Research, 2017

Would you be interested in a solution that unifies all endpoint management?



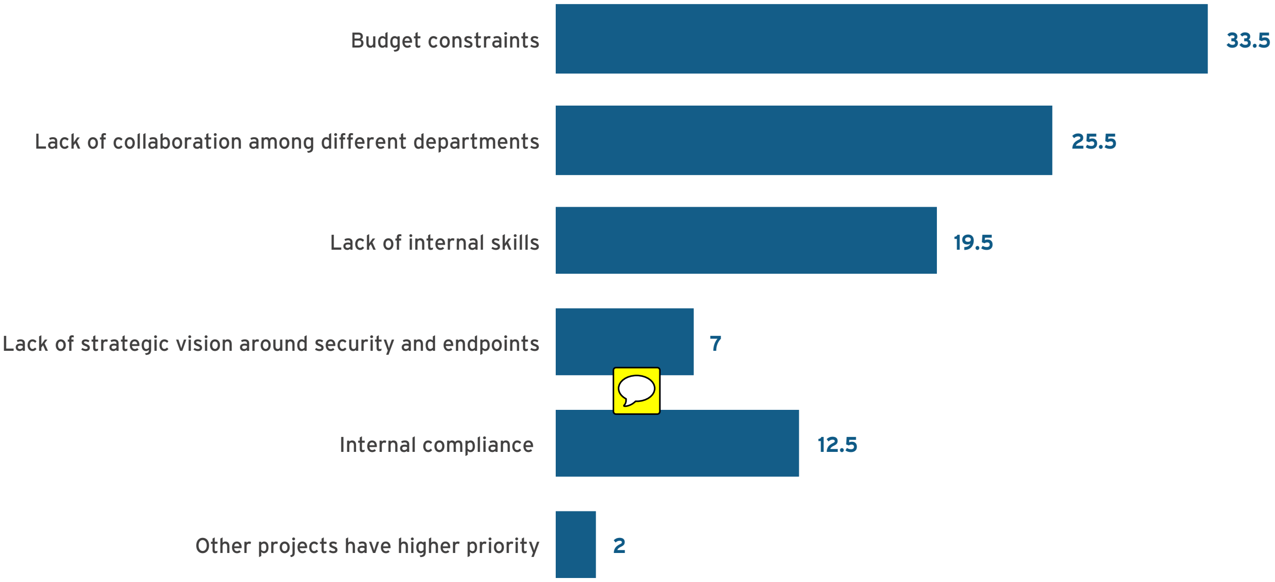
UNIFED ENDPOINT CHALLENGES

For many companies, the combination of potentially flat or decreasing budgets and the complexity of siloed traditional endpoint and IoT endpoint stacks – each with its own developer and lifecycle management tools, protocols and middleware – create many barriers to entry. When we asked about the perceived barriers to more mature endpoint strategies, respondents cited budget constraints as the top barrier. The focus on budget constraints could serve as a reminder for unified endpoint management vendors to clarify the ROI and TCO propositions of integrated approaches, especially in the context of legacy platform investment. (See Figure 8.)

Figure 8: Budgets and lack of internal collaboration hold back endpoint maturity

Source: 451 Research, 2017

What do you see as the obstacles to becoming more mature with your endpoint strategy?

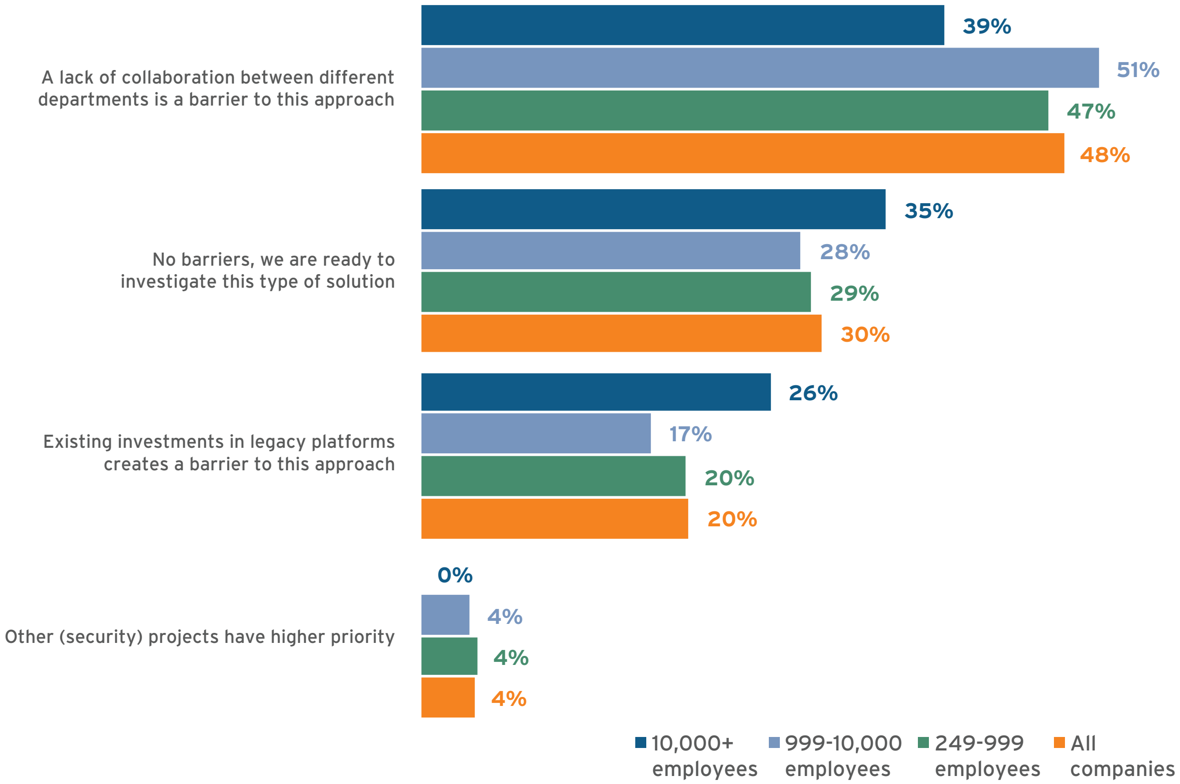


Drilling into the topic one step further, we asked the question 'Do you foresee barriers to bringing traditional endpoint security together with IoT security and management to a unifed platform to govern all endpoints?' There was both good and bad news for unified platform vendors.

On one hand, 30% of total respondents indicated that they are ready to investigate a unified solution immediately – that is clearly the good news. The bad news is that even more respondents view the lack of collaboration among different departments as an inhibitor to this approach. The takeaway for vendors is that unified endpoint sales cycles could be long and will require a selling effort that extends beyond IT stakeholders to include targeting the C suite. Enterprise leaders should revisit their own organizations and take steps to remove such barriers through appointing a C-level project champion, setting up cross-disciplinary teams or common platforms. The goal is to remove the barriers in the way of aligning business goals with IT investments. (See Figure 9.)

Figure 9: Lack of internal collaboration could hold back unified endpoint security and management

Source: 451 Research, 2017



Other Findings

When we asked about information security threats, the top three were clear. The top two threats that responsdents cited originate from outside of the organization. The low incidence of perceived threats from insider-based attacks could indicate a false sense of security regarding internal security practices.

Figure 10: What security threats are firms least prepared for?

Source: 451 Research, 2017

Threat	Percentage
Hackers with malicious intent	32%
Cyberwarfare	29%
Compliance	21%
Internal audit deficiencies based on findings	11%
Insider espionage	7%

We also asked respondents to identify where decisions were made in the organization around mobility and IoT. The conclusion is that while IT will continue to be heavily involved, other groups will also have input and responsibilities. We suggest that having ultimate oversight reside within IT makes good strategic sense given the need for OT systems to be integrated and secured within the corporate IT infrastructure.

Figure 11: Which business units are responsible for mobility, IoT and endpoint tasks?

Source: 451 Research, 2017

	Led by IT	Led by LOB	Led by combination of LOB, OT and IT	Led by OT
Strategy for how the organization leverages mobility and IoT	70%	17%	22%	6%
Budget for endpoint security	37%	38%	30%	15%
IoT management and governance	49%	26%	38%	8%
IoT device security	45%	30%	26%	26%
Worker mobility security and governance	38%	23%	44%	15%
Strategy for securing the various mobile hardware and software assets	47%	28%	34%	14%
Responsibility for compliance where it may be impacted by endpoint security	47%	25%	40%	14%
Responsibility for adhering to regulatory requirements	38%	31%	37%	14%

Although it is interesting that compliance ranked so high here, this can be attributed to the survey including highly regulated markets such as financial services and healthcare. That said, it's a stark reminder of how damaging the failure to meet compliance responsibilities can be for an organization. Concerns about damaged repution and loss of trust also ranked highly. Clearly, a security breach can bring untold costs in terms of brand erosion and lost of trust internally and externally that can take months or years to repair.

Figure 12: Concerns about endpoint security

Source: 451 Research, 2017

Threat	Percentage
Failing compliance responsibilities	34%
Damaging our reputation among employees and partners	20%
Losing the trust of customers	19.5%
Losing or publicly exposing sensitive data	16.5%
Losing intellectual property	9%

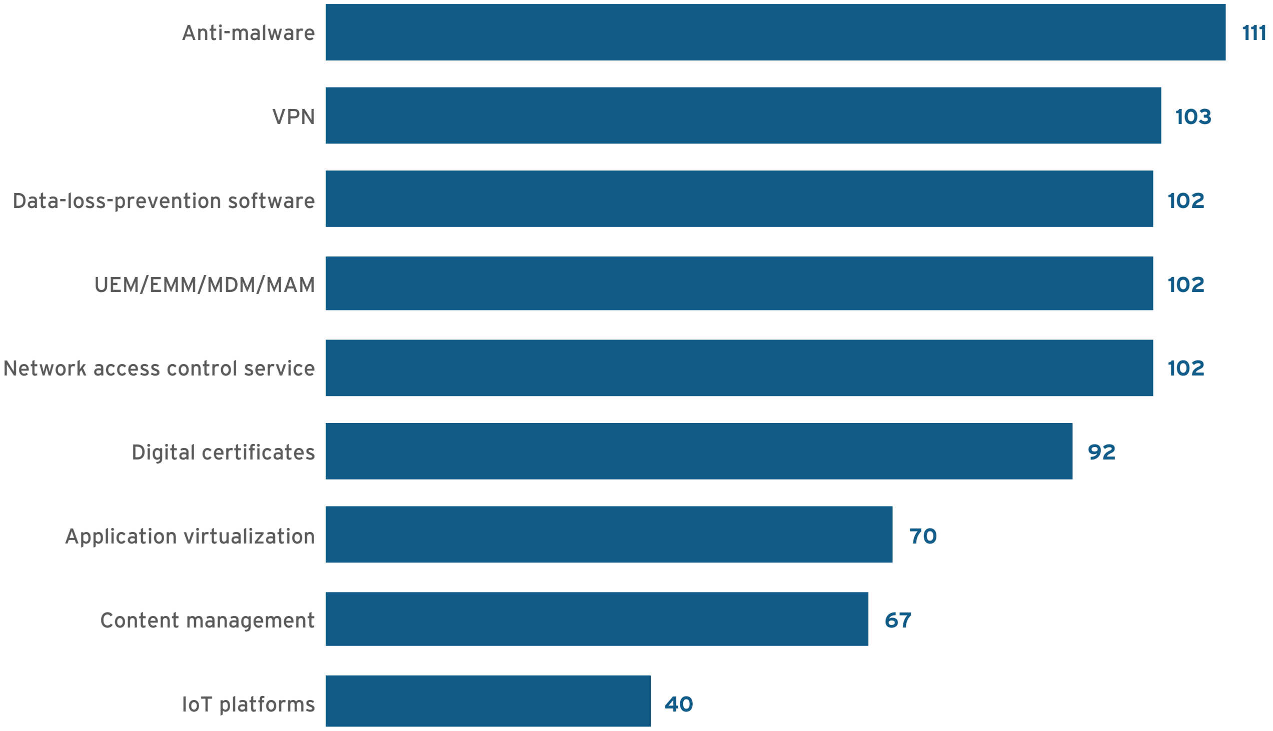
Looking at the technologies currently in place to mitigate risks around endpoint data, all participants (100%) reported that their organizations have deployed at least one type of solution. However, they typically use more than one; a majority (90%) report using eight or more of the technologies listed (See Figure 13).

The most widely used technologies are anti-malware, VPN, data loss prevention software, and the combination of UEM/EMM/MDM/MAM with at least 50% of respondents using these.

Most organizations will rely on multiple solutions, which will result in greater complexity in the deployment of IoT initiatives. This can be explained – at least in part – by the fact that the most widely used solutions tend to be legacy technologies that have been used for traditional endpoint management. Newer technologies – including IoT platforms – are not widely used to mitigate risks. This indicates that organizations have not yet identified a single solution that can address the multiple risks around endpoint data.

Figure 13: Technologies deployed to mitigate risks around endpoint data

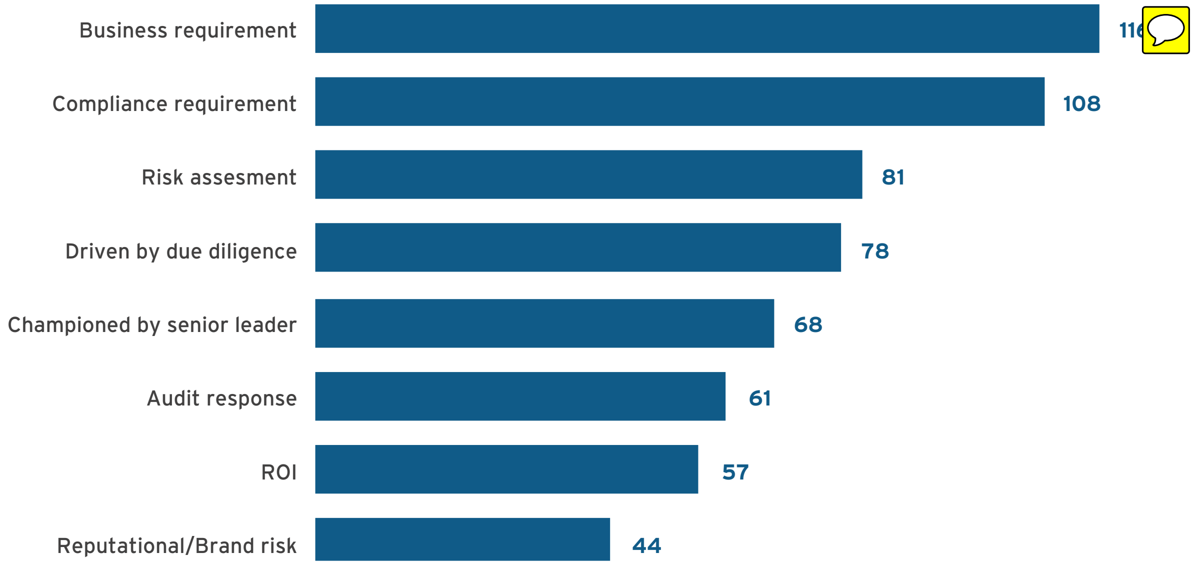
Source: 451 Research, 2017



Given the correlation between endpoint security concerns and compliance cited in Figure 12 above, it makes sense that 'compliance requirement' is the second most popular factor cited for receiving approval for security projects among respondents. The fact that ROI was far down the list of responses is telling – it only takes one major breach to bring a firm to its knees, and calculating ROI is difficult for security products that work as they should.

Figure 14: Factors cited for approving security projects

Source: 451 Research, 2017



Conclusion

It makes little sense to consider traditional endpoint security and management and emerging IoT programs as definitively separate initiatives. Leaders, especially those not too far down the path with legacy technologies, have the opportunity to bring IoT and enterprise worker digital initiatives together; they face the same challenges and create opportunities to leverage experience and learning in one to apply to the other. Bringing these initiatives under one 'roof' will create cost efficiencies by leveraging common platforms and will also require organizations to cross the internal chasms – both technical and cultural – between OT and IT departments.

Security has been and will continue to be the first concern for organizations when considering IoT investments, just as it has been with BYOD initiatives for employee work. However, security is often a tough ROI sell because when things are going right, it goes largely unnoticed, yet a security failure can cause untold damages – both direct and indirect. Bringing both the responsibility and management tools into a centralized function will ensure consistency in approach and the ability to rapidly respond to incidents that might arise.

Vertical industries such as financial services and healthcare share several requirements, which make them excellent candidates for unified endpoint management for application management, security and governance. These requirements include the need to manage multiple human and machine assets, a need to continuously look for ways to optimize supply-chain processes, a requirement to act quickly on operational intelligence, and the criticality of governance for health and safety, quality assurance and auditing.