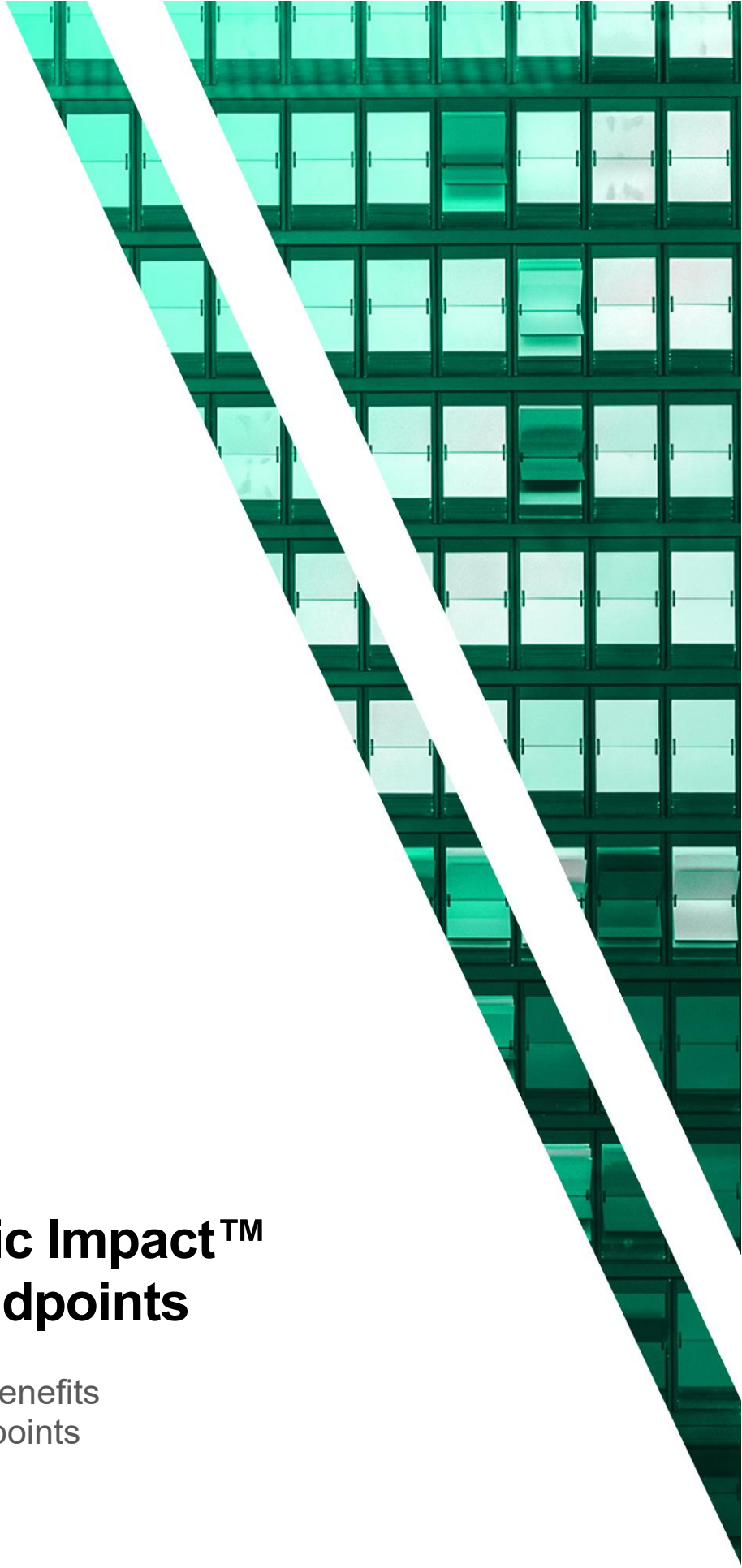
FORRESTER®



The Total Economic Impact™ Of Modernizing Endpoints

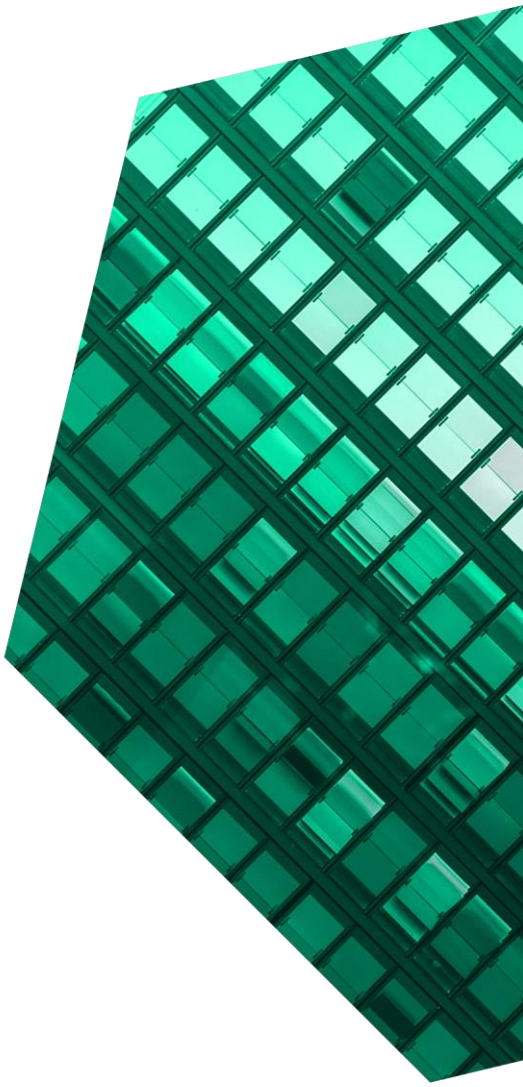
Cost Savings And Business Benefits Enabled By Modernizing Endpoints

SEPTEMBER 2021

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY MICROSOFT

Table Of Contents

Project Lead: *Kim Finnerty*



ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

Executive Summary

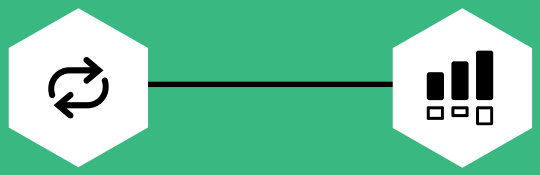
In 2020, firms became aware of the need for modernizing the way they monitor and maintain of the increasing number and type of endpoints their employees use to complete their jobs successfully. Modernizing endpoints involves several types of solutions and offers wide-ranging benefits across the organization from better security to improved employee productivity and increased sales revenue.

The term “modernizing endpoints” refers to the evolution of procuring, deploying, and managing endpoints for users, enabling those users for hybrid work, and providing secure and simple access for employees on any device. This is primarily achieved by adopting a cloud-first model for deployment and management, and moving the focus of security from the local network to the endpoint itself. Throughout this study, the term “endpoints” may refer to desktops, laptops, notebooks, tablets, virtual desktops, mobile phones, and a whole array of specialized devices for use in settings from hospitals to warehouses to retail stores to concert venues.

Microsoft commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by modernizing their endpoint management approach.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of transforming their digital estate by modernizing their endpoints across their organization.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four decision-makers and surveyed 301 decision-makers with experience modernizing their endpoints. For the purposes of this study, Forrester aggregated the experiences of the interviewed and surveyed decision-makers and combined the results into a single composite organization.

KEY STATISTICS



Return on investment (ROI)
284%

Net present value (NPV)
$20.90M

Prior to modernizing endpoints, the interviewees’ organizations used multiple vendors and platforms to manage and protect endpoints and their employees’ activity. However, prior attempts to improve monitoring and reporting yielded limited success, leaving organizations with an ever-growing array of solutions that needed coordination. These limitations led to interest in a single-vendor, integrated solution to enable both the usefulness and security of endpoints.

KEY FINDINGS

Quantified benefits. Risk-adjusted present value (PV) quantified benefits include:

- **Enhanced end-user experience delivered $7.7 million to the organization.** Modern endpoint management protects the organization while untethering employees from the local network. They can work anywhere and at any time, and do so at least as productively as they would in the

office, thus improving both satisfaction and productivity.

- **Avoided security risk saved the organization $3.8 million.** Automated and centralized control of endpoints ensured better compliance at each endpoint and, thus, allowed the organization to maintain effective security despite a significant shift to remote and hybrid work.
- **Increased IT productivity delivered nearly $16.2 million in savings.** Modernization of endpoints reduces complexity for the IT team significantly. In addition, automation and integration reduced the need for IT to do time-consuming manual tasks, such as imaging and provisioning machines, changing passwords, and updating applications.
- **Eliminated redundant solutions resulted in more than $607,000 in reduced costs.** Modernizing endpoints allowed organizations to shed other point solutions and consolidate on fewer solutions, saving organizations licensing fee and vendor support costs.

Unquantified benefits. Benefits that are not quantified for this study include:

- **Increased customer delight**. Consistently functional and responsive endpoints allow frontline workers (FLW) to improve customer experience. Doing so kept customer and guest interactions moving to reduce customer abandonment, discharged patients expeditiously, allowed employees to fill warehouse orders accurately, and scan tickets quickly at events.
- **Improved collaboration between IT and other organizational functions**. As work became more distributed and employees moved to remote working, business units turned to IT to set up virtual collaboration. IT also worked more closely with security operations because of the security benefits of modernizing endpoints, increasing collaboration between IT and other departments.
- **Avoided reputational damage.** Interviewees noted that modernizing their organizations' endpoints protected their organizations from potential security risks stemming from remote access from data breaches to a lack of compliance with government regulations or industry norms. Interviewees were particularly concerned that these events could have devastating long-term impacts on their organizations' reputations.

Costs. Risk-adjusted PV costs include:

- **Subscription to Microsoft's E3 and F3 licenses, costing $2.1 million.** Access to the tools available in the Microsoft E3 and F3 licenses enables the integration of endpoint performance and security that defines a modern endpoint.
- **Implementation costs of nearly $4.8 million.** IT support was required to install and operationalize the tools to optimize endpoint functionality and security. Some organizations also needed to replace or upgrade a significant number of devices to ensure compatibility with modern endpoint security software.
- **Additional IT training for employees, costing $472K.** Some organizations introduced new training for employees so they can get the most out of the new endpoint management approach."

The financial analysis which is based on the decision-maker interviews and survey found that a composite organization experiences benefits of $28.3M over three years versus costs of $7.4M, adding up to a net present value (NPV) of $20.9M, and an ROI of 284%.

ROI
284%

BENEFITS PV
$28.26M

NPV
$20.90M

PAYBACK
<6 months

Benefits (Three-Year)

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews and survey, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in modernizing endpoints.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that modernizing endpoints can have on an organization.

Forrester Consulting conducted an online survey of 351 cybersecurity leaders at global enterprises in the US, the UK, Canada, Germany, and Australia. Survey participants included managers, directors, VPs, and C-level executives who are responsible for cybersecurity decision-making, operations, and reporting. Questions provided to the participants sought to evaluate leaders' cybersecurity strategies and any breaches that have occurred within their organizations. Respondents opted into the survey via a third-party research panel, which fielded the survey on behalf of Forrester in November 2020e

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Microsoft and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in modernizing endpoints.

Microsoft reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

Microsoft provided the customer names for the interviews but did not participate in the interviews.

Forrester fielded the double-blind survey using a third-party survey partner.

DUE DILIGENCE

Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to modernizing endpoints.

DECISION-MAKER INTERVIEWS AND SURVEY

Interviewed five decision-makers at four organizations which had modernized endpoints with Microsoft and surveyed 301 IT executives to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewed and surveyed decision-makers.

FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interviews and survey using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the decision-makers.

CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

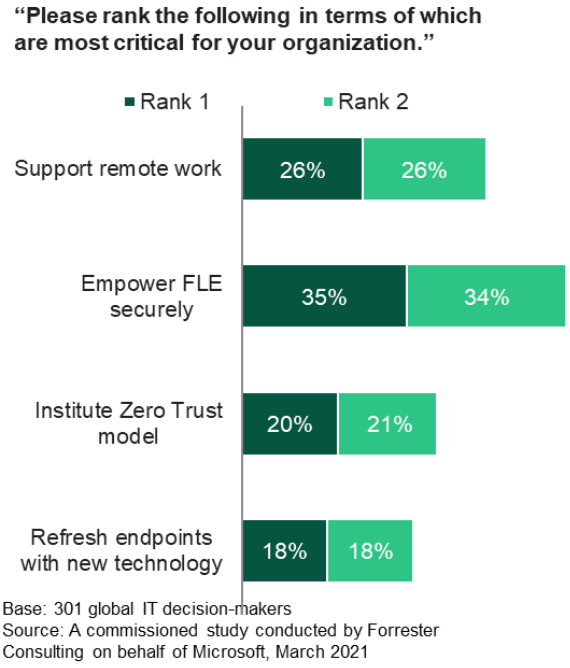
The Customer Journey to Modernizing Endpoints

Drivers leading to the investment in modernizing endpoint

KEY CHALLENGES

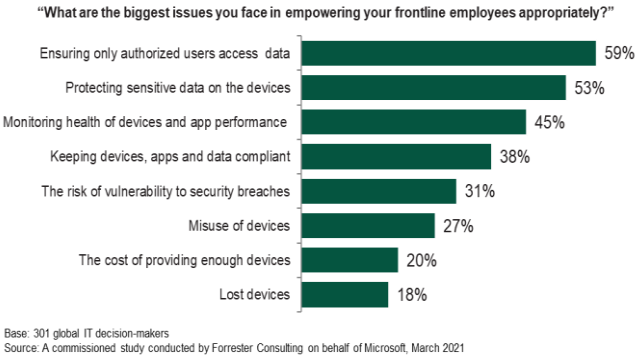
New challenges are facing organizations due to long-term business trends which accelerated during the COVID-19 pandemic. As more workers and more data have shifted from secure enterprise networks to endpoints, it has become more difficult—and more critical—for organizations to secure and manage those endpoints. Forrester interviewed five decision-makers at four organizations and surveyed 301 IT executives with experience modernizing their organizations' endpoints. For more details on the organizations that participated in this study, see Appendix B.

Before modernizing their organizations' endpoints, most of the interviewees were focused on securing their organizations' networks, partly by restricting employee access to it. They used an array of tools such as VPN, GPOs (Group Policy Objects), and device-specific endpoint solutions from multiple vendors to facilitate remote work on both corporate and non-corporate endpoints.



The decision-makers noted that their organizations struggled with common challenges, including:

- **Meeting the technology needs of frontline workers.** The top priority among surveyed IT decision-makers was to provide the necessary technology that makes today's frontline workforce productive and happy. These devices sped up service at point of sale, enabled package tracking, kept manufacturing lines running, and ensured healthcare workers had up-to-date patient information at shift change. They were critical to these workers' ability to do their jobs.



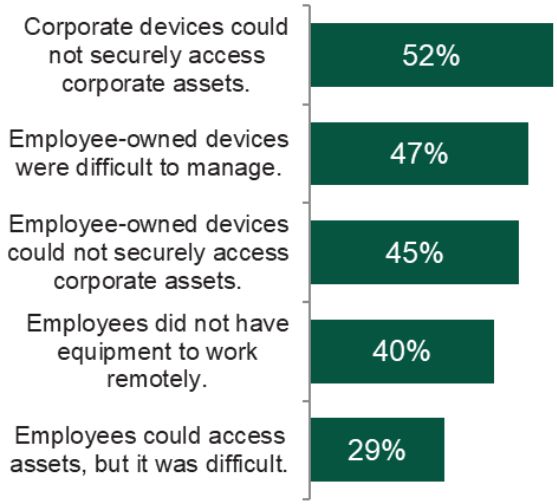
Although many of the devices frontline workers use were specialized and did not require access to all corporate data and resources, they were still needed to connect to corporate applications and databases. Due to their exclusive use in non-corporate locations, as well as the fact that workers on different shifts often shared devices, these endpoints were vulnerable. Protecting these devices without undermining them was a high priority.

- **An urgent, growing mandate to enable secure remote work.** The COVID-19 pandemic accelerated a long-term trend toward more mobile work for employees who were previously in a corporate office and used devices that the office secured. As more firms differentiated themselves and built customer loyalty by providing in-person, on-site, and/or 24-hour services to customers, their employees needed secure yet simple access to the data and tools they would normally use in the office. Surveyed

decision-makers found that, during COVID-19, their organizations' existing endpoint security approach made it difficult for both end users and IT professionals to manage remote work and employee-owned devices (BYOD).

Employers were also under pressure to improve employee satisfaction and reduce turnover by allowing people to use their own devices and work with more flexibly between home and office, all while maintaining productivity. Interviewees noted that remote working flexibility was fast becoming an expectation in the workplace, so IT must make it work seamlessly.

"What were your biggest challenges in keeping employees productive during the COVID-19 pandemic?"



Base: 301 global IT decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, March 2021

- **Growing pressure to secure their organizations' digital estate with a Zero Trust security model.** Surveyed decision-makers said their organizations were not quite one-third of the way to operating with a Zero Trust model on average, although it is their third highest priority.

  Modernizing an organization's endpoints is an integral element in achieving a Zero Trust methodology, as it is the only way to ensure that all devices and the apps they run, no matter where they are or who owns and manages them, are verifiable before they access corporate data assets.

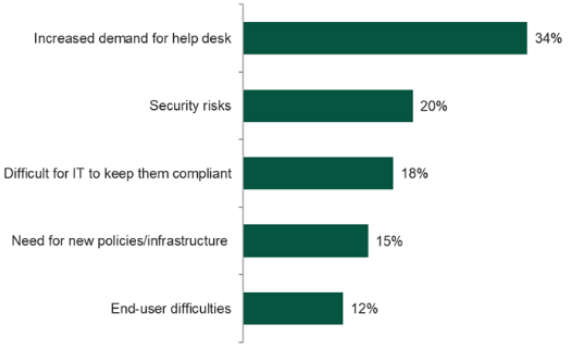
"Where would you say your company is on the journey to implementing a Zero Trust security model?"

Base: 301 global IT decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, March 2021

- **The need to provide all employees with the most up-to-date technology possible.** Survey respondents placed this need fourth overall, but over one-third of them rated it first or second in priority. Updates and upgrades are a way of life for technology products, and respondents want to ensure that their employees have access to the best. For some, it is a critical competitive advantage.

  Interviewees told Forrester that modernizing their organizations' endpoints pushed out updates quickly and easily, whether for security purposes or to take advantage of new capabilities. It also facilitated device refreshes and new operating system or other major installs. The CTO at a professional services organization stated: "When

What is the biggest challenge you face in bringing next generation devices to your organization?



Base: 301 global IT decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, March 2021

> we replace [laptops], all we do is send the kit out and the thing pretty much builds itself."

Based on the interviews and survey, Forrester constructed a TEI framework, a composite organization, and a ROI analysis that illustrates the areas financially affected. The composite organization is representative of the five decision-makers (at four organizations) that Forrester interviewed and the 301 decision-makers that Forrester surveyed. It is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics.

Description of composite. The composite organization is a healthcare provider that makes $1 billion in annual revenue and employs a total of 4,000 people, including approximately 1,500 office/knowledge workers (including management) and 2,500 frontline healthcare workers in the field.

The knowledge workers at the company generally use at least two endpoints: a laptop computer and a company-owned mobile device. Frontline employees use both shared tablets and their personal mobile phones. A small number of research technicians and physicians use advanced scientific devices that also access the hospital's data

Key assumptions

- **$1 billion revenue**
- **Healthcare provider**
- **4,000 employees**
- **Multiple endpoint types**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Improved end-user experience	$3,087,162	$3,087,162	$3,087,162	$9,261,486	$7,677,315
Btr	Avoided security risk	$1,534,173	$1,534,173	$1,534,173	$4,602,519	$3,838,103
Ctr	Increased IT productivity	$6,499,235	$6,499,235	$6,499,235	$19,497,705	$16,162,635
Dtr	Eliminated redundant solutions	$244,161	$244,161	$244,161	$732,483	$607,191
	Total benefits (risk-adjusted)	$11,364,731	$11,364,731	$11,364,731	$34,094,193	$28,225,289

IMPROVED END-USER EXPERIENCE

Evidence and data. Employee experiences interacting with technology on the job are a key factor in their level of job satisfaction. Whether they are corporate executives or frontline workers, they want to see technology enabling their success, not frustrating them and hindering their work. Employees who can easily complete their tasks — no matter where they are — are happier, more productive employees.

> **"We are becoming a mobile, globally distributed workforce, and this supports a strategic imperative to interact with clients anytime, anywhere."**
> *CTO, professional services*

- A CTO at a professional services organization said: "When I first came to the organization, I did the rounds asking people what they thought of our technology. Predominantly people said, 'Our tech is rubbish. It doesn't work. The laptops don't work. We don't like it.' I don't hear any of that now."
- A director of user services and security operations at a pharmaceutical organization said: "The value proposition to the end user is in terms of consistency of use and being able to work anywhere on their laptop, the same way they do in the office."

Modeling and assumptions. Several assumptions underlie Forrester's model of this benefit's value.

- All 4,000 employees use some type of endpoint that requires some level of access to corporate data and applications.
- On average, employees use their devices during 70% of their working hours.
- Devices run, on average, 2% faster after modernization with fewer agents in place on them.
- The average fully burdened hourly wage across the organization is $33.40.
- It takes an average of 2 hours per laptop and 30 minutes per mobile or FLW endpoint for IT to

repair or update devices, and 60% of employees experience that need each year.

- The average organization recaptures 65% of the time saved in productive work.

Risks. The risk that other organizations may experience value on a different magnitude varies with the following factors:

- The amount of time employees power up and use their devices during the workday.
- The frequency and duration of downtime related to network and IT access issues.
- The average wage of device users.
- The extent to which the organization can recapture time saved.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $7.7 million.

Improved End-User Experience

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Employees using endpoints	Composite	4,000	4,000	4,000
A2	Average fully burdened hourly wage	Industry sources	$33.40	$33.40	$33.40
A3	Average hours saved with fewer agents running on endpoints	Assumption	27	27	27
A4	Average hours saved waiting for IT intervention (updates, etc.)	Assumption	1.5	1.5	1.5
A5	Hours saved with faster power up	Assumption	11	11	11
A6	Value of end-user hours saved	(A5+A4+A3)*A1*A2	$5,277,200	$5,277,200	$5,277,200
A7	Percent recaptured	Assumption	65%	65%	65%
At	Improved end-user experience	A6*A7	$3,430,180	$3,430,180	$3,430,180
	Risk adjustment	↓10%			
Atr	Improved end-user experience (risk-adjusted)		$3,087,162	$3,087,162	$3,087,162
	Three-year total: $2,261,486			**Three-year present value: $7,677,315**	

AVOIDED SECURITY RISK

Evidence and data. Interviewees told Forrester that there were multiple ways in which their organizations' modernized endpoints have improved security for them. The endpoints were more likely to be in compliance with their organizations' security protocols than they were before. This is because patches and updates were automatically pushed to the devices and required virtually no effort on the part of the end user.

Interviewed decision-makers also commented that modern endpoints were more likely to have a standard set of applications installed on them either during the provisioning process or through a companywide rollout. That consistency allowed them to have more security around managing their environment.

Additionally, most interviewees felt that many of their organizations' existing endpoint management processes were out of date or lacking in some way.

For instance, a CTO at a professional services organization stated: “The actual application lifecycle — so the provisioning, the licensing, the patching, feature releases, and the retirement — was a bit fragmented and a bit ad hoc, and there were policies that needed reviewing that did not fit the purpose anymore.”

The interviewees noted that their organizations’ focus on securing the endpoint and not just the network perimeter moved them towards a goal of operating with a Zero Trust security model. It ensured that all devices and the applications on them, no matter where they were or who owned and managed them, were verifiable before they accessed corporate data assets

“We recently had a ransomware scare. But very quickly—within minutes—we put in blocks to IP addresses that would have been involved and we were able to crush it.”
Director, user services and security operations, pharmaceuticals

Modeling and assumptions. To model the value of this benefit to the composite organization, Forrester assumes:

- The out-of-pocket cost of the average breach for the organization is $242,540.[2] This includes everything from internal costs to identify and remediate the breach to external costs such as legal expenses and brand damage repair.
- Each breach causes 3.5 hours of lost productivity per employee.[3]
- The average breach affects 20% of knowledge workers and 10% of FLW.[4]
- The composite organization is likely to experience 2.5 such breaches per year.[5]
- The degree of risk added by the organization’s shift to remote working and more sophisticated FLW devices is assumed to be similar to the massive increase in cybercrime activity seen since the COVID-19 pandemic.[6]
- The organization avoids virtually all of this increased risk by modernizing their endpoints.

Risks. The risk that organizations experience a different value for this benefit is related to:

- Any variation in the actual cost of breach based on specific industry conditions.
- Differences in the amount of likely incremental risk added and avoided based on previous security strength.

To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted benefit of $3.8 million.

Avoided Security Risk					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Out-of-pocket cost of security breach	Forrester research	$242,540	$242,540	$242,540
B2	Hours of lost productivity per employee	Forrester research	3.5	3.5	3.5
B3	Employees affected per breach	1,500*20%+2,500*10%	550	550	550
B4	Average fully burdened hourly salary	Industry sources	$33.40	$33.40	$33.40
B5	Cost of lost productivity per breach	B2*B3*B4	$64,295	$64,295	$64,295
B6	Average breaches per year	Forrester research	2.5	2.5	2.5
B7	Usual expected security breach costs	(B1+B5)*B6	$767,087	$767,087	$767,087
B8	Incremental risk from remote work, avoided by modernizing endpoints	Assumption	$1,917,716	$1,917,716	$1,917,716
Bt	Avoided security risk	B8	$1,917,716	$1,917,716	$1,917,716
	Risk adjustment	↓20%			
Btr	Avoided security risk (risk-adjusted)		$1,534,173	$1,534,173	$1,534,173
	Three-year total: $4,602,519		**Three-year present value: $3,815,262**		

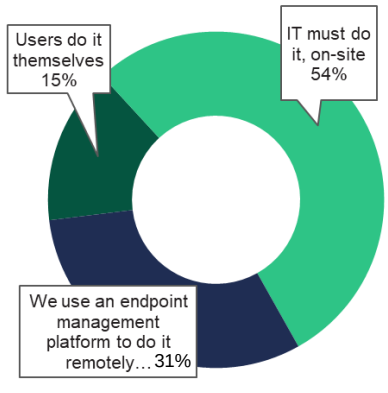
INCREASED IT PRODUCTIVITY

Evidence and data. The new realities of remote working and increased FLW connectivity created greater complexity for IT teams as they need to monitor and support multiple types of shared and physically distributed devices. For most of the surveyed decision-makers, this work falls to the IT team to handle at a central site

Interviewees noted, however, that modernizing their organizations' endpoints with Microsoft greatly simplified this task because of its integrated approach to end-to-end management of the endpoints. This both provides end users with self-service solutions, and provides IT with a single, cohesive endpoint management solution.

- The CTO at a professional services organization said: "One of the big self-service items was resetting passwords on endpoints. People always seem to not be able to reset their password on weekends and holidays."

"How do you keep endpoints provisioned, updated, and secured?"



Base: 301 global IT decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, March 2021

Modeling and assumptions. In order to model the value of this benefit for the composite organization, Forrester assumes:

- The organization redeploys 60% of its pre-modernization IT time to more value-added tasks and projects than resetting passwords and provisioning devices.
- The fully burdened average wage of an IT team member is $49.22.
- The organization eliminates approximately 90% of its provisioning-related help desk tickets.
- The cost per incident of those help desk tickets is $15.56.

Risks. The risk that other organizations will not achieve the same type of benefits as the composite is related to:

- The number of hours IT spends provisioning, updating, and ensuring compliance for remote endpoints before modernizing.
- The amount of time IT spends providing help desk support related to remote access, identity verification, and other problems associated with remote devices trying to access corporate data.
- The salary of IT team members.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted PV (discounted at 10%) of $16.2 million.

“We definitely have fewer tickets; we almost never get the ‘blue screen of death’ or hardware-related tickets anymore.”
Director of IT, healthcare

Increased IT Productivity					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Endpoint management hours before modernizing endpoints	Interviews	240,000	240,000	240,000
C2	Endpoint management hours after modernizing endpoints	Assumption	96,000	96,000	96,000
C3	Average fully burdened network engineer salary	Industry sources	$49.22	$49.22	$49.22
C4	Endpoint management FTE redeployment savings	(C1-C2)*C3	$7,087,680	$7,087,680	$7,087,680
C5	Helpdesk provisioning-related tickets per year before modernization	24,000/year*40%	9,600	9,600	9,600
C6	Provisioning-related tickets per year after modernization	14,400/year*7%	1,008	1,008	1,008
C7	Cost per incident	Industry sources	$15.56	$15.56	$15.56
C8	Helpdesk ticket reduction savings	(C5-C6)*C7	$133,692	$133,692	$133,692
Ct	Increased IT productivity	C4+C8	$7,221,372	$7,221,372	$7,221,372
	Risk adjustment	↓10%			
Ctr	Increased IT productivity (risk-adjusted)		$6,499,235	$6,499,235	$6,499,235
	Three-year total: $19,497,704		**Three-year present value: $16,162,635**		

ELIMINATED REDUNDANT SOLUTIONS

Evidence and data. Interviewees pointed out that the move to modernizing their organizations' endpoints was not just about using more modern software. It allowed them shed other point solutions and use fewer solutions as a whole, because of Microsoft's unified management and integrated cloud solutions. Eliminating redundant solutions not only saved the organizations licensing or per user fees associated with the software, but also the maintenance contracts and/or IT time devoted to keeping the solutions updated.

- The director of user services and security operations at a pharmaceutical organization noted: "I only want to buy one license for things. I don't want to buy two licenses for the same capability. So, why would I pay for an E3 or E5 license and then another license for something else?"

Modeling and assumptions. To model the value of this benefit to the composite organization, Forrester assumes:

- The organization retires two point solutions it previously used to secure the network perimeter.
- Each solution cost $100,000 in annual licensing fees, as well as a 20% vendor maintenance agreement.
- Each solution also requires 10% of a system administrator's time to monitor and maintain.

Risks. The value organizations may see from this benefit will be impacted by:

- The number and cost of point solutions the modernization of the organization's endpoints made redundant.

- The size, complexity, and cost of the organization's connectivity infrastructure before moving to a modern endpoint environment.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted benefit of $607,191.

Eliminated Redundant Solutions

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Number of software licenses	Interviews	2	2	2
D2	Average annual fees per license	Interviews	$100,000	$100,000	$100,000
D3	Vendor maintenance contracts	D1*D2*20%	$40,000	$40,000	$40,000
D4	On-site administrator hours	Industry Sources	384	384	384
D5	Fully burdened system administrator average hourly wage	Industry Sources	$44.30	$44.30	$44.30
Dt	Eliminated redundant solutions	(D1*D2)+D3+(D4*D5)	$257,011	$257,011	$257,011
	Risk adjustment	↓5%			
Dtr	Eliminated redundant solutions (risk-adjusted)		$244,161	$244,161	$244,161
	Three-year total: $732,482		**Three-year present value: $607,191**		

"We want our users focused on the patient. Every minute they're focused on an IT problem is a minute they are not focused on the patient."
Director of user services and security operations, pharmaceuticals

UNQUANTIFIED BENEFITS

Interviewees identified a number of benefits that had a major impact on their organizations, but that they were unable to quantify.

- **Increased customer delight**. Modernizing endpoints increased frontline workers effectiveness, allowing those workers to deliver the kind of customer experience that can be a true competitive advantage.
  - The VP and chief information security officer (CISO) at a retail organization said: "Providing the right endpoint for our frontline workers lets them move from 'I'm going to sit behind a cash register and ring up transactions' to 'I'm going to meet the customer where they are in the store, engage with them, and solve their problems.'"
- **More effective collaboration between IT and other functions.** Several interviewees spoke about a change in the way IT works with other functions. As work became more distributed and employees moved to remote working at the start of the pandemic, business units turned to IT to set them up for virtual collaboration both

internally and with customers. The IT teams' ability to do this with Office 365 and modern endpoints has created more of a partnership between IT and the business. A similar dynamic has taken place with security operations, where IT has delivered strong security instead of higher vulnerability with distributed access to corporate data.

- **Avoided reputational damage**. Interviewees expressed concern about different types of reputational damage, depending on their industry. For some, the concern was over meeting accepted professional standards; for others, it was a matter of legal and regulatory compliance. Many decision-makers also mentioned the threat of dissatisfied customers amplified by social media.
    - The director of information technology at a healthcare organization said: "We have 130 people in our contact center, and if they could not pick up their laptops and go home during the COVID-19 pandemic, there could have been a significant impact to our ability to provide patient service. One bad comment out there can perpetuate and prevent you from getting additional business."

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement modernized endpoints and later realize additional uses and business opportunities.

Interviewees noted that their organizations' investments in modernizing endpoints put them in a position to be opportunistic and use market and social events to their advantage. While they spoke primarily about using the changes brought about by the COVID-19 pandemic as a springboard to advance or cement their progress, the decision-makers agreed that their organizations' improved state of readiness is will likely help in a similar way when another unforeseen event comes along.

"The investments we made in Microsoft cloud-based services so we can extend to any device are what put us in a position to really leverage the disruption of COVID-19 to do true digital transformation."
Director of user services and security operations.

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Etr	Software license cost	$0	$856,800	$856,800	$856,800	$2,570,400	$2,130,735
Ftr	Implementation costs	$2,625,000	$525,263	$1,050,525	$1,050,525	$5,251,313	$4,759,999
Gtr	Additional IT training	$420,840	$20,369	$20,369	$20,369	$481,946	$471,494
	Total costs (risk-adjusted)	$3,045,840	$1,402,431	$1,927,694	$1,927,694	$8,303,658	$7,362,218

SOFTWARE LICENSE COST

Evidence and data. Microsoft 365 E3 and F3 licenses provided decision-makers with the tools necessary to modernize their organizations' endpoints, along with access to the full Office 365 suite of products.

- Microsoft Endpoint Manager (MEM) offered the flexibility to comanage endpoints via the cloud with Intune and on-premises via Configuration Manager.
- Windows Autopilot allowed IT teams to preconfigure, reset, repurpose, and recover devices with little-to-no infrastructure.
- Azure Active Directory (AAD) provided seamless access to applications from a wide range of devices and locations.
- M365 Defender protected, coordinated defense, and supported proactive hunting across the system.

These solutions allowed the interviewees' organizations to connect all of their endpoints more securely to corporate resources with less disruption to the end-user experience.

The organizations whose executives were interviewed for this study had already purchased the required licenses (or better) for some or all of their employees to provide them with access to Windows and Office 365 functionality. In these cases, no additional investment would be required for those employees for whom a license was already purchased. Forrester conservatively assumes that all employees at the composite organization require a Microsoft license.

Modeling and assumptions. Forrester assumes the following:

- The composite organization has 1,500 knowledge workers who require an E3 license, and 2,500 frontline workers who require an F3 license.
- The E3 license is $32/month and the F3 is $8 month.
- The organization buys one appropriate license for each employee, which covers multiple endpoints per employee (e.g., a laptop and mobile phone or a tablet and medical device).

Risks. The primary risks that another organization's licensing costs will vary:

- The overall number of incremental licenses required.
- The mix of license types required.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 5%) of $2.1M.

Software License Cost						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Enterprise E3 license	Assumption		$384	$384	$384
E2	E3 Users	Assumption		1,500	1,500	1,500
E3	F3 license	Assumption		$96	$96	$96
E4	F3 users	Assumption		2,500	2,500	2,500
Et	Software license cost	(E1*E2)+(E3*E4)	$0	$816,000	$816,000	$816,000
	Risk adjustment	↑5%				
Etr	Software license cost (risk-adjusted)		$0	$856,800	$856,800	$856,800
	Three-year total: $2,570,400			**Three-year present value: $2,130,735**		

IMPLEMENTATION COSTS

Evidence and data. Interviewees noted that, beyond the licensing fees, their organizations had additional expenses involved in modernizing their endpoints. One of the largest of these was the need to update the actual hardware their employees were using. Many interviewees reported their organizations had previously used a "sweat the asset" approach to hardware refreshes. As part of their commitment to modernizing endpoints, they instituted a three- or four-year cycle of hardware updates. This generally resulted in a significant upfront cost as they replaced hardware that was already out of date, and then experienced an ongoing cost to keep employees supplied with up-to-date technology

The interviewees reported their organizations' IT, and in some cases, executive teams spent time and money on associated projects to get the maximum benefit from the organizations' modern endpoint investments. These included re-evaluating and rewriting policies, processes, and standards for managing the environment going forward.

Modeling and assumptions. Forrester's valuation of this benefit assumes:

- The composite organization spends $1 million before launch in project costs.
- The organization institutes a three-year refresh cycle for its endpoints and purchases 1,334 new devices each year.
  - Each device costs an average of $750.
  - The composite organization replaces 2,000 devices upfront to update legacy equipment and provide several months of breathing room in Year 1.

Risks. The following factors may impact these costs:

- The time devoted to the prelaunch projects.
- The salaries of the personnel involved in the projects.

- The number of devices an organization buys each year.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $4.8M.

Implementation Costs

Ref.	Metric	Source	Initial	Ye4.8ar 1	Year 2	Year 3
F1	Project costs	Interviews	$1,000,000			
F2	Upgrade out-of-date hardware	Interviews	$1,500,000	$500,250	$1,000,500	$1,000,500
Ft	Implementation costs	F1+F2	$2,500,000	$500,250	$1,000,500	$1,000,500
	Risk adjustment	↑5%				
Ftr	Implementation costs (risk-adjusted)		$2,625,000	$525,263	$1,050,525	$1,050,525
	Three-year total: $5,251,313			**Three-year present value: $4,759,989**		

ADDITIONAL EMPLOYEE IT TRAINING

Evidence and data. While the interviewees reported their organizations' investments in modern endpoints provided important advantages to end users, they also involved different usage routines for end users. As a result, some organizations introduced additional employee training to ensure that employees knew how to get the most out of the capabilities the new endpoint management approach offered.

Modeling and assumptions. For this cost, Forrester assumes:

- The composite organization introduces a robust technology learning module for all current and incoming employees, so they know how to make sure their endpoints remain in compliance.
- The one-time training requires 3 hours of employee time.
- The average companywide wage is $33.40.

Risks. The impact of this cost may vary based on:

- The length and breadth of the endpoint training.
- The rate of turnover/new hires per year.
- The average wage of people taking the training.

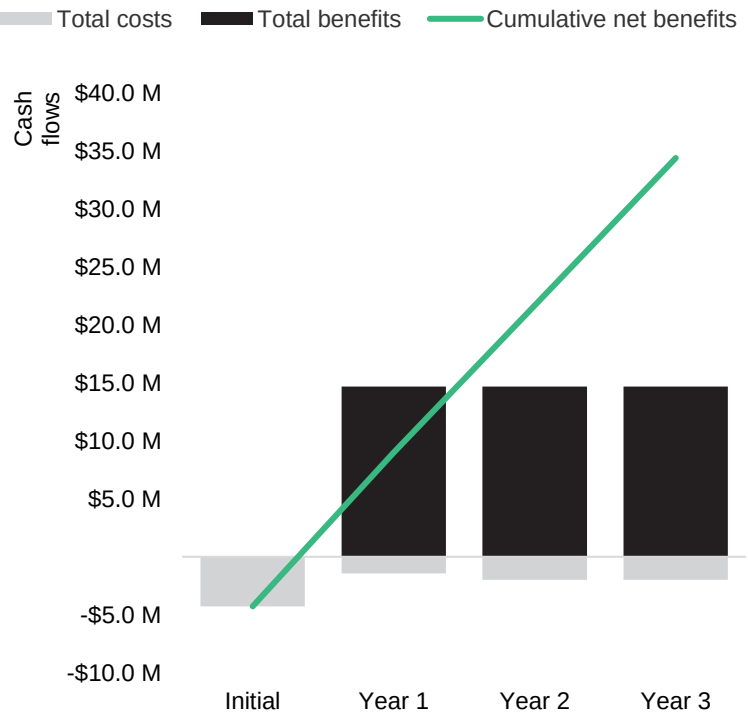
To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $472,000.

Additional Employee IT Training						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	Employee turnover per year	Industry Sources		22%	22%	22%
G2	New employees hired per year	C1*H1	4,000	880	880	880
G3	Average hourly fully burdened salary	Industry Sources	$33.40	$33.40	$33.40	$33.40
G4	Hours IT training per new employee	Interviews	3	3	3	3
Gt	Additional IT training	G1*G2*G3*G4	$400,800	$19,399	$19,399	$19,399
	Risk adjustment	↑5%				
Gtr	Additional IT training (risk-adjusted)		$420,840	$20,369	$20,369	$20,369
	Three-year total: $481,946			**Three-year present value: $471,494**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($3,045,840)	($1,402,431)	($1,927,694)	($1,927,694)	($8,303,658)	($7,362,218)
Total benefits	$0	$11,364,731	$11,364,731	$11,364,731	$34,094,193	$28,262,403
Net benefits	($3,045,840)	$9,962,299	$9,437,037	$9,437,037	$25,790,533	$20,900,185
ROI						284%
Payback period (months)						<6

Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

TOTAL ECONOMIC IMPACT APPROACH

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

PRESENT VALUE (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

NET PRESENT VALUE (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

PAYBACK PERIOD

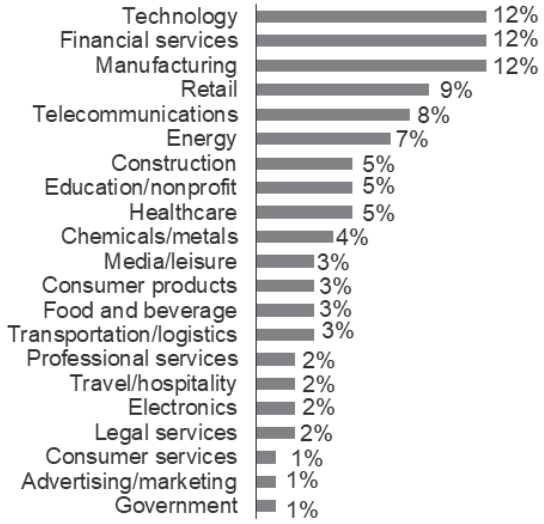
The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendix B: Interview And Survey Demographics

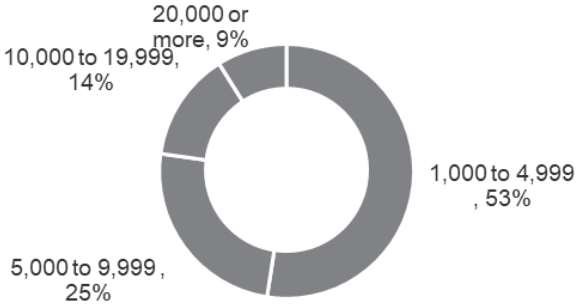
Interviewed Decision-Makers			
Interviewee	**Industry**	**Region**	**Size**
Director, information technology IT IS program director	Healthcare	Headquartered in the US	1,000 employees
CTO	Professional services	Headquartered in the UK	3,750 employees
Director, user services and security operations	Pharmaceutical	Headquartered in the US	1,000 employees and 500 contractors
VP chief information security officer	Retail	Headquartered in the US	40,000 employees

Survey Demographics

INDUSTRIES



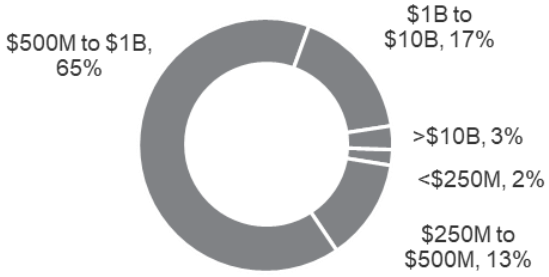
SIZE



REGION

26%	Canada
25%	United States
14%	Germany
13%	France
13%	United Kingdom
10%	Australia

REVENUE



Base: 301 global IT decision-makers
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, March 2021

Appendix C: Endnotes

[1] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.
[2] Source: Forrester Consulting Cost of a Cyberbreach Survey, Q4 2020.
[3] Source: Ibid
[4] Source: Ibid
[5] Source: Ibid
[6] Source: "Top Cyber Security Exports Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic," PR Newswire, August 11, 2020 (https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html).


FORRESTER®