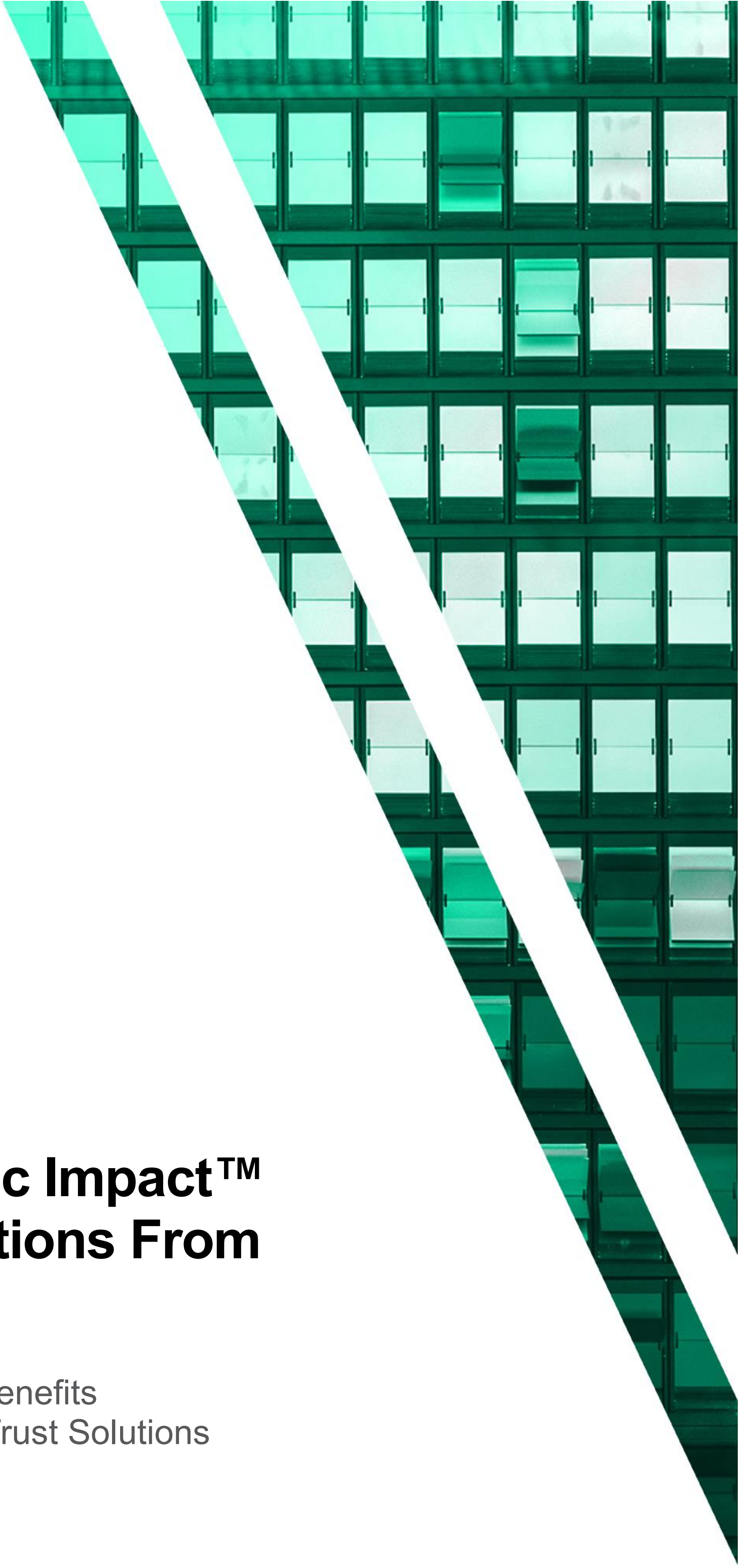
FORRESTER®



The Total Economic Impact™ Of Zero Trust Solutions From Microsoft

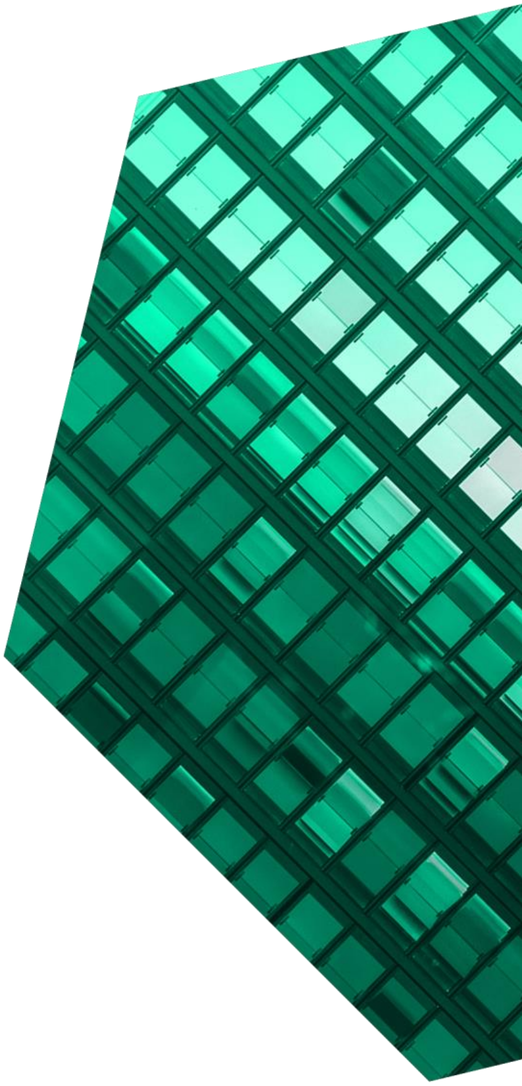
Cost Savings And Business Benefits Enabled By Microsoft's Zero Trust Solutions

DECEMBER 2021

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY MICROSOFT

Table Of Contents

Consulting Team: Edgar Casildo
Benjamin Corey



Executive Summary

Information security leaders face growing security challenges as digital estates continue to grow in complexity, their organizations adapt to the realities of hybrid work, and they face an increase in ransomware and sophisticated cyberattacks. By using Microsoft solutions to implement a Zero Trust architecture, organizations can improve their security posture, increase organizational agility, and empower their employees.

Zero Trust is a proactive, integrated approach to security across all digital layers that explicitly and continuously verifies every transaction, asserts least privilege, and relies on intelligence, advanced detection, and real-time response to defend against threats. When implementing Zero Trust, organizations should adhere to the following principles:

- **Explicitly verify.** Security decisions should be made using all available data points, including identity, location, device health, resource, data classification, and anomalies.

- **Use least-privilege access.** Access should be limited with both just-in-time/just-enough-access (JIT/JEA) and risk-based adaptive policies.

- **Assume breach.** Blast radius should be minimized with microsegmentation, end-to-end encryption, continuous monitoring, and automated threat detection and response.

Microsoft enables organizations to implement a comprehensive Zero Trust strategy that spans identities, devices, apps, network, infrastructure, and data through a robust portfolio of integrated security solutions—including solutions for identity and access management (IAM), endpoint management, cloud security, threat protection, network security, and more. Together, these tools enable organizations to simplify their cybersecurity strategy and retire unnecessary legacy solutions while improving their security posture.

KEY STATISTICS

Return on investment (ROI)
92%

Net present value (NPV)
$11.6M

Microsoft commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by implementing a Zero Trust framework with Microsoft solutions.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of implementing a Zero Trust architecture with Microsoft for their organizations.

To better understand the benefits, costs, and risks associated with implementing a Zero Trust architecture with Microsoft solutions, Forrester interviewed eight decision-makers at five organizations undergoing Zero Trust journeys. Forrester aggregated the interviewees' experiences and combined the results into a single composite organization for this study.

Interviewees said that prior to adopting a Zero Trust architecture, their organizations used myriad legacy solutions to stitch together security strategies for compliance purposes. These approaches made the organizations too dependent on VPNs and left them with outdated identity management solutions, inadequate device management controls, and insufficient visibility into their corporate networks. These limitations led to increased risks of data breaches, restrictive authentication policies that hurt the employee experience (EX), and challenges with onboarding new technology and employees.

Since the investment in implementing a Zero Trust architecture, the interviewees' organizations have rolled out policies and technologies to improve their security postures, simplify security management, increase employee productivity, and enable greater business agility. Key results from these investments include reducing the risks of a data breach, improving the productivity of end users and IT, and improving security management processes.

KEY FINDINGS

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

- **Reduced spend from legacy software and infrastructure by over $7 million.** The composite organization saves $20 per employee per month by eliminating now-redundant security solutions, including, endpoint management, antivirus, and antimalware solutions.

  Additionally, interviewees said their organizations could retire significant amounts of on-premises software and hardware, such as legacy IAM solutions. As the organizations continued to implement a Zero Trust architecture with Microsoft's cloud-based products and services into their ecosystems, more opportunities to retire legacy solutions arose, which led to increased savings year over year.

- **Accelerated the process to set up end users on new devices by 75%.** Interviewees said they reduced the time required to set up end users on new devices by connecting apps to Microsoft Azure AD, enabling single sign-on (SSO) and multifactor authentication (MFA). Because setups are faster and more efficient, end users needed less help in the weeks following setup.

- **Reduced the number of security and IAM-related help desk calls by 50%.** Connecting applications to Azure AD for SSO and MFA makes it easier for users — especially remote workers — to access the applications they need; this reduces the number of submitted application support tickets.

  In addition, the composite organization also experiences fewer false positive security alerts and faster cross-domain remediation, saving security teams time. In a related study, Forrester found that Microsoft Sentinel can reduce the number of false positives by 79%.[2] And interviewees in another study said that when security incidents did occur, Microsoft Defender could automatically detect and remediate over 90% of security incidents, preventing the spread of a security attack.[3]

- **Reduced the effort required to provision and secure new infrastructure by 80%.** Interviewees said the management capabilities built into Microsoft solutions helped their organizations implement robust cloud governance strategies as part of their Zero Trust journeys. This involved standardizing workflows and automating routine tasks like provisioning and securing new resources.

  The time required to provision new infrastructure went from taking several months to mere days. This not only allowed IT teams to support business users at the speed of business, but it also improved their organizations' overall security postures.

- **Reduced the resources required for audit and compliance management by 25%, saving $2 million.** The built-in advanced audit and discovery capabilities, like those in the centralized Microsoft 365 compliance center, make it easier for security and compliance personnel in the composite organization to audit their environment and understand the policies they need to implement to comply with internal and external governance requirements. Additionally, because the composite organization has consolidated under the Microsoft platform, its security team can enforce policies faster and more consistently with less effort than before.

- **Increased the efficiency of security teams by 50%.** Interviewees said Microsoft 365 Defender helped their organizations triage alerts, correlate additional threat signals, and take remediation actions. Additionally, migrating key security solutions to the cloud freed up time previously spent on system updates and other operational tasks.
- **Frontline workers gained access to business-critical applications and systems of record, saving more than three business days per year.** Interviewees said enabling SSO and bring-your-own-device (BYOD) practices reduced friction for employees to access their organizations' apps. This allowed them to perform essential tasks even while in the field, which reduced the need to return to headquarters or a centralized location. Interviewees at a logistics firm noted that seasonal workers benefited tremendously from this shift. Seasonal workers could now access critical applications; this eliminated the need to pair them with full-time workers and allowed them to work independently, resulting in significant efficiency gains.
- **Enhanced security reduced the risk of a data breach by 50%.** Microsoft solutions helped organizations improve authentication, network, and endpoint security protocols. When coupled with increased visibility into the network, the interviewees' organizations reported they were better able to protect themselves from data breaches. Additionally, increased segmentation of the networks also meant that the organizations experienced diminished financial losses when a breach did occur.

  The interviewees said their organizations improved their security postures and mitigated the possibility of a data breach arising from compromised credentials, phishing attacks, cloud misconfigurations, compromised business emails, social engineering, vulnerabilities in third-party software, and malicious insiders. These initial attack vectors were responsible for 80% of the data breaches in 2021.[4] By reducing the possibility and impact of a data breach from any one of these attack vectors, the interviewees' organizations reduced the possibility of a data breach in general.

> **"The great thing [about our Zero Trust journey] is that we've strengthened our security greatly while making it easier for our end users to do their jobs."**
> *Principal architect of information security, logistics*

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

- **Allowing to transition from capex to opex.** Because Microsoft's solutions are software-as-a-service (SaaS)-based, organizations can quickly expand or contract their environments without needing to purchase additional hardware or dedicating resources to implement changes.

> **Our doctors and nurses are really busy saving lives. What we’re trying to do is get technology out of the way. Adding passwordless [authentication] and unifying access is going to help them focus more on their patients while keeping them more secure.**
>
> — Executive director of information services, healthcare

Recurring monthly charges also offer a cash-flow benefit over up-front licensing.

- **Reducing the likelihood of regulatory fines.** Implementing a Zero Trust architecture helps organizations adhere to a wide range of regulatory requirements and reduces the number of noncompliance penalties they could incur.

Costs. Risk-adjusted PV costs include:

- **Initial implementation and planning costs of $1.5 million.** The composite organization dedicates internal resources to deploy Microsoft’s offerings and the retirement of its legacy solutions. The composite organization also engages with a Microsoft partner to create an adoption roadmap, assist in deploying the various Microsoft workloads, and conduct adoption and change management workshops.
- **Incremental Microsoft licensing costs of $4.5 million over three years.** Forrester quantified the incremental cost of upgrading 50% of the composite organization’s knowledge workers to Microsoft 365 E5 licenses and 50% of its frontline workers to Microsoft 365 F3 licenses. Forrester also quantified the additional costs associated with leveraging more of Microsoft’s solutions as part of the composite organization’s Zero Trust strategy.
- **Ongoing management costs of $5.3 million.** The composite organization dedicates internal resources to manage its Microsoft solution stack.
- **Additional bandwidth investment of $410,000.** The composite organization invests in additional bandwidth to accommodate the increased network demands.
- **Internal training costs of $756,000.** Forrester quantified the internal labor costs associated with training the composite organization’s workforce on the new policies and solutions.

The decision-maker interviews and financial analysis found that a composite organization experiences benefits of $24.1 million over three years versus costs of $12.6 million, adding up to a net present value (NPV) of $11.6 million and an ROI of 92%.

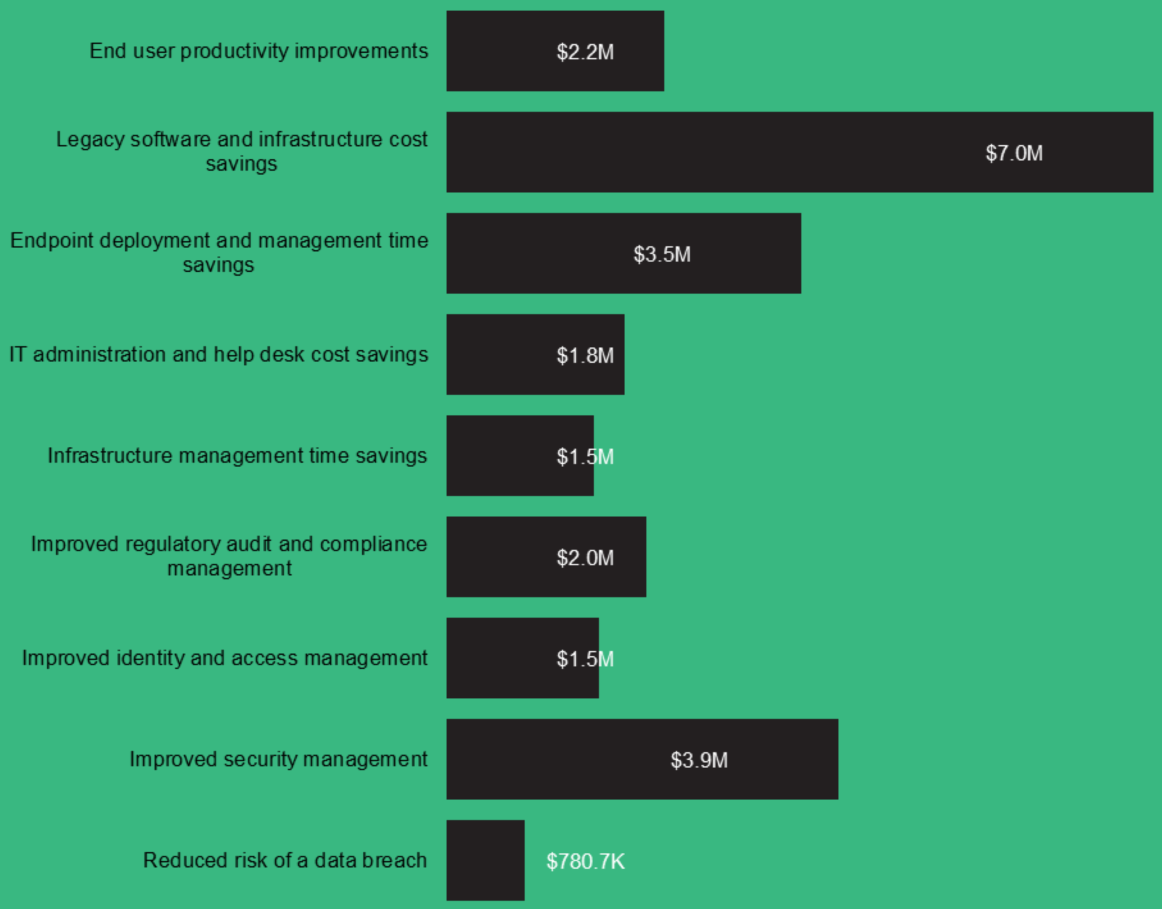
ROI
92%

BENEFITS PV
$24.1M

NPV
$11.6M

PAYBACK
<6 months

Benefits (Three-Year)



TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in using Microsoft solutions to implement a Zero Trust architecture.

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 Microsoft solutions can have on an organizations Zero Trust journey.

DUE DILIGENCE

Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to the solutions from Microsoft that enable Zero Trust.

DECISION-MAKER INTERVIEWS

Interviewed eight decision-makers at five organizations using Microsoft solutions for their Zero Trust journeys to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees' organizations.

FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interviews 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.

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 Microsoft to adhere to Zero Trust strategies.

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.

The Zero Trust Solutions From Microsoft Customer Journey

Drivers leading to the Microsoft Zero Trust solutions investment

Interviewed Decision-Makers

Interviewee	Industry	Region	Employees
Senior IT officer	Financial service	Global	20,000+
Senior information security officer	Financial service	Global	20,000+
Solutions architect	Manufacturing	Global	60,000+
Identity engineer	Manufacturing	Global	60,000+
Principal architect of information security	Logistics	Global	400,000+
Principal architect of technical service	Logistics	Global	400,000+
Executive director of information services	Healthcare	North America	150,000+
Enterprise security architect	Energy	EMEA	10,000+

KEY CHALLENGES

The interviewees noted how their organizations struggled with common challenges.

- **Proactive remediation and threat reduction was difficult with prior solutions.** Existing security solutions failed to provide the high-fidelity signals, comprehensive visibility, and end-to-end self-healing capabilities needed to defend against today’s sophisticated attackers and the volume of cyberthreats. Their prior solutions could not provide telemetry of a threat’s effect on data, a user’s exact activity on the network, or a timeline for effective remediation. Additionally, because the organizations used security solutions from numerous vendors, consolidating telemetry information for triage and analytical work was difficult and time-consuming.

- **IAM teams struggled to manage their environments while empowering end users.** Interviewees said their organizations’ legacy infrastructures made it difficult for IAM teams to meet organizational security requirements and the needs of their users. The legacy infrastructures were difficult to maintain and prone to downtime, leaving little time to address growing security expectations. These systems also failed to support the organizations’ changing security needs. For example, interviewees at a manufacturing firm noted that their organization’s legacy IAM systems failed to meet regional legal requirements, and they prevented the organization from rolling out MFA to a significant portion of its workforce. Meanwhile, users (especially remote workers) struggled to remember all of the access methods and passwords they needed for various applications.

- **Complying with regulatory requirements was difficult.** Interviewees said the complexity of their organizations’ IT environments made it difficult to audit their environments or effectively implement governance policies. Decision-makers wanted to find a way to make it easier to comply with these requirements.

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the interviewees' organizations, and 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 based in the United States and its operations are global. It has 10,000 employees: Half are knowledge workers, and half are frontline workers. All knowledge workers have Microsoft 365 E5 licenses, and all frontline workers have Microsoft 365 F3 licenses.

The composite organization's knowledge workers had a combination of Microsoft 365 E3 and E5 licenses prior to beginning its Zero Trust journey. Meanwhile, only half of the organization's frontline workers had any type of desktop license, and many relied entirely on paper processes to perform day-to-day tasks. The composite organization also used a combination of on-premises and SaaS security solutions.

Deployment characteristics. The composite organization adopts most of the security products under Microsoft 365 E5—including Azure Active Directory, Microsoft Defender 365, Microsoft Information Protection and Governance, Insider Risk Management, and more—as well Microsoft Sentinel and Microsoft Defender for Cloud.

Key assumptions

- **Global operations**
- **10,000 employees**
- **5,000 employees have Microsoft 365 E5 licenses**
- **5,000 employees have Microsoft 365 F3 licenses**

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	End user productivity improvements	$602,333	$982,800	$1,066,000	$2,651,133	$2,160,709
Btr	Legacy software and infrastructure cost savings	$2,565,000	$2,755,000	$3,230,000	$8,550,000	$7,035,424
Ctr	Endpoint deployment and management time savings	$1,405,915	$1,420,165	$1,434,414	$4,260,494	$3,529,491
Dtr	IT Administration and help desk cost savings	$551,000	$744,800	$874,000	$2,169,800	$1,773,095
Etr	Infrastructure management time savings	$233,280	$794,880	$794,880	$1,823,040	$1,466,203
Ftr	Improved regulatory audit and compliance management	$708,750	$850,500	$850,500	$2,409,750	$1,986,204
Gtr	Improved identity and access management	$405,000	$648,000	$810,000	$1,863,000	$1,512,284
Htr	Improved security management	$1,406,250	$1,577,813	$1,755,675	$4,739,738	$3,901,451
Itr	Reduced risk of a security breach	$233,722	$333,178	$389,832	$956,731	$780,714
	Total benefits (risk-adjusted)	$8,111,250	$10,107,135	$11,205,301	$29,423,686	$24,145,575

END USER PRODUCTIVITY IMPROVEMENTS

Evidence and data. The interviewees said that by implementing Zero Trust architecture, their organizations improved EX and increased productivity. The interviewees noted that they increased device performance and stability by managing all of their endpoints with Microsoft Endpoint Manager (MEM); consolidating their endpoint management stacks reduced the number of agents installed on end users' devices. Forrester found that these actions can reduce boot times from taking 30 minutes to less than a minute for some organizations.[5]

Implementing Zero Trust increased productivity by empowering employees with the choice to work from anywhere with any device as long as they properly authenticated on a compliant device and app.

For example, a principal architect of technical services in the logistics industry said their organization recognized security improvements that allowed it to create a BYOD program for seasonal frontline workers. This led to significant efficiency gains. The interviewee said: "Before, our seasonal workers would have to be paired with our full-time employees when [performing field visits]. But now [that we allow BYOD], they can go out on their own [to perform field visits]." These changes enabled the seasonal frontline workers to be much more productive than before.

Moreover, the shift to Zero Trust reduced the burden of security away from end users. Implementing SSO and MFA, leveraging passwordless authentication, and eliminating VPN clients reduced day-to-day friction and improved end user productivity.

In a related study about Microsoft 365 E5, interviewees said leveraging the management capabilities offered by Microsoft 365 E5 significantly benefited remote workers.[6] One interviewee said: "[We] probably spent 25% more time supporting remote workers than the office workers. Now that we have a standard suite of tools that can be controlled and managed across endpoints and geographies, we've seen a reduction in the support needs of our remote workers."

Relevant products:

- **Microsoft Endpoint Manager**
- **Microsoft Defender for Endpoint**
- **Azure Active Directory**
- **Azure AD Conditional Access**

Another interviewee in that study said their organization experienced a 40% decrease in the number of support tickets submitted by remote workers.[7]

Modeling and assumptions. Forrester assumes the following about the composite organization:

- Seamless SSO, passwordless authentication, and eliminating VPN solutions save the composite organization's end users 10 minutes per week.
- Connecting applications to Azure AD for SSO and MFA makes it easier for users (especially remote workers).
- Field service employees can now access important business applications and data on either company-owned devices or their personal devices, enabling them to support customers and complete field visits faster than before.
- The composite organization improves knowledge worker productivity by eliminating cumbersome security controls (e.g., passwords, VPNs) and improving device performance by reducing the number of security agents that run on a device.

- The productivity capture rate of knowledge workers is 50% because not all time savings translate into additional value-add work.

Risks. Forrester recognizes that end user productivity improvements may vary by organization depending on:

- Preexisting solutions and productivity benchmarks.
- The number of employees at an organization and average labor rates.
- Cultural and organizational change management barriers.

Results. To account for risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $2.2 million.

End User Productivity Improvements

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Frontline workers	Composite	5,000	5,000	5,000
A2	Time saved per week due to efficiency gains from increased access to business applications, passwordless authentication (hours)	Interviews	0.25	0.5	0.5
A3	Frontline worker average hourly salary	TEI Standard	$25	$25	$25
A4	Frontline worker annual time savings	A1*A2*52 weeks *A3	$1,625,000	$3,250,000	$3,250,000
A5	Knowledge workers	Composite	5,000	5,000	5,000
A6	Weekly time savings from Azure AD SSO, passwordless authentication, and other process improvements	Interviews	10	12	15
A7	Efficiency gain per user (hours)	A6/60 minutes* 52 weeks	8.7	10.4	13.0
A8	Average hourly knowledge worker rate	TEI Standard	$32	$32	$32
A9	Knowledge worker productivity gains	A5*A7*A8	$1,386,667	$1,664,000	$2,080,000
A10	Productivity recapture	Assumption	25%	25%	25%
At	End user productivity improvements	(A4+A9)*A10	$752,917	$1,228,500	$1,332,500
	Risk adjustment	↓20%			
Atr	End user productivity improvements (risk-adjusted)		$602,333	$982,800	$1,066,000
	Three-year total: $2,651,133	**Three-year present value: $2,160,709**			

LEGACY SOFTWARE AND INFRASTRUCTURE COST SAVINGS

Evidence and data. By deploying Zero Trust solutions from Microsoft, the interviewees' organizations could consolidate their spending on SaaS security software and retire on-premises security solutions. Interviewees reported eliminating on-premises IAM solutions, VPN software, and third-party antivirus, antimalware, and security information and event management (SIEM) solutions.

- The principal architect of technical services at the logistics firm said: "We've been able to move our employee portal and all the applications behind that — as well as our third-party SaaS applications — to Azure Active Directory. This enabled us to retire our legacy on-premises IAM solution. We've been able to reallocate employees from maintaining our legacy IAM systems to migrating the remainder of our applications to Azure AD."
- A senior information security officer in the financial services industry said: "Before, we had on-premises legacy systems that needed to be replaced. These systems weren't being patched or maintained properly. These systems were a big risk, yet nobody could make the case that we should spend the money to replace them since they were working fine. But now that we're moving towards Zero Trust, we can justify retiring legacy systems as part of a broader digital transformation effort. Over time, efforts like this will allow us to shrink our data centers."
- In a related Forrester TEI study, the head of cybersecurity for a natural resources company stated, "Our prior solutions were not giving us an accurate picture. That left us vulnerable to material risks, which isn't a good thing for a public company." [8]

Modeling and assumptions. Forrester assumes the following about the composite organization:

Relevant products:

- **Azure**
- **Azure AD**
- **Microsoft Endpoint Manager**
- **Microsoft Defender for Endpoint**
- **Microsoft Sentinel**
- **Microsoft Defender**
- **Azure Security**
- **Microsoft Defender for Cloud Apps**

- The composite organization replaces its previous antivirus, mobile device management (MDM), and threat detection solutions with those offered through Microsoft.
- The average monthly user savings for security tools is $20.
- The composite organization previously incurred $1 million in additional costs related to its legacy VPN, IAM, and SIEM solutions. This included the costs of software licenses, on-premises hardware, and log ingestion and storage fees. Over time, the composite organization is able to eliminate the software license agreements for each of these services and their associated infrastructures.

Risks. Forrester recognizes that legacy software and infrastructure cost savings may vary by organization depending on:

- The organization's size and its ability to negotiate discounts.
- The costs associated with legacy security solutions.

- The amount of infrastructure that is on-premises.
- The degree to which the organization adopts Microsoft security solutions.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $7.0 million.

Legacy Software And Infrastructure Cost Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Users	Composite	10,000	10,000	10,000
B2	Per-user monthly security tools license cost	Interviews	$20	$20	$20
B3	Spend on security infrastructure	Interviews	$300,000	$500,000	$1,000,000
Bt	Legacy software and infrastructure cost savings	B1*B2*12 + B3	$2,700,000	$2,900,000	$3,400,000
	Risk adjustment	↓5%			
Btr	Legacy software and infrastructure cost savings (risk-adjusted)		$2,565,000	$2,755,000	$3,230,000
		Three-year total: $8,550,000		Three-year present value: $7,035,424	

ENDPOINT DEPLOYMENT AND MANAGEMENT TIME SAVINGS

Evidence and data. By using Microsoft security solutions, included in Microsoft 365 E5, like Microsoft Endpoint Manager (MEM) and Azure AD, the interviewees' organizations modernized endpoint management and made it easier for IT to manage devices. This allowed end users to set up their devices faster, increasing productivity.

- Interviewees said connecting applications with Azure AD, enabling SSO and MFA, and migrating to SharePoint enabled end users to get up and running on new devices much faster than they could before, which reduced the frequency of support tickets. Meanwhile, Conditional Access and the configuration capabilities within MEM reduced the extra configuration work IT administrators had to perform to address department- or user-specific needs.

- Interviewees said their organizations recognized time savings regardless of device, and they said it's easy to manage myriad mobile devices, PCs, and Macs. That management is now mostly automated.

- The principal architect of technical services at the logistics firm said the benefits offered by adopting Zero Trust principles reduced the technical support end user needed and reduced the time and costs associated with onboarding and off-boarding employees. They said: "We no longer have to set up [seasonal workers] with a device, issue them a [security software] token, configure our VPN software, and support all that hardware and software. This is really important for seasonal workers who are onboarded very quickly — sometimes just a few hours before they need to start making deliveries."

Relevant products:

- **Azure AD**
- **Microsoft Endpoint Manager**
- **Azure AD Conditional Access**

Modeling and assumptions. Forrester assumes the following about the composite organization:

- The fully loaded hourly salary of an IT employee is $58.

- The fully loaded hourly salary of an end user is $32.

- Before using Microsoft's solution stack, the composite required an hour to set up a new endpoint and six hours to configure a new user laptop.

- Microsoft's endpoint management solutions reduce endpoint configuration times by 75%.

Results. To account for variances between organizations, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $3.5 million

Endpoint Deployment And Management Time Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Time spent configuring new endpoints (hours) (rounded)	10,000 employees/3*1 hour	3,333	3,333	3,333
C2	Reduced endpoint configuration due to 365	C1 * 75%	2,500	2,500	2,500
C3	Time required to setup a user on a new laptop before 365 (hours)	Interviews	6	6	6
C4	IT end user setup time savings	C1*C3*75%	14,999	14,999	14,999
C5	End user setup time savings	C1*C3*75%	14,999	14,999	14,999
C6	IT staff member fully loaded hourly salary	Assumption	$58	$58	$58
C7	End user fully loaded hourly salary	Assumption	$31	$32	$33
C8	**Total IT time savings**	**(C2+C4)*C6**	**$1,014,942**	**$1,014,942**	**$1,014,942**
C9	**End user savings**	**C5*C7**	**$464,969**	**$479,968**	**$494,967**
Ct	Endpoint deployment and management time savings	C8+C9	$1,479,911	$1,494,910	$1,509,909
	Risk adjustment	↓5%			
Ctr	Endpoint deployment and management time savings (risk-adjusted)		$1,405,915	$1,420,165	$1,434,414
	Three-year total: $4,260,494		**Three-year present value: $3,529,491**		

IT ADMINISTRATION AND HELP DESK COST SAVINGS

Evidence and data. Interviewees said a major benefit of implementing a Zero Trust architecture with Microsoft was a reduction in help desk calls and shortened ticket resolution times.

- Remote workers benefited significantly from the new management methods and experienced fewer performance and access issues than before. As a result of these improvements, one interviewee said their organization experienced a 40% decrease in support tickets submitted by remote workers.

- The principal architect of technical services for the logistics firm said: “Shifting to Azure AD for authentication greatly reduced the number of issues we experience. It was very hard for us to scale authentication with our previous infrastructure. Previously, if there were a problem with authentication, application teams would have to be intimately involved in remediating that issue. In comparison, we don’t have any authentication issues for the applications we’ve moved to Azure AD.”

Modeling and assumptions. Forrester assumes the following about the composite organization:

- Each user makes an average of eight help desk calls a year related to forgotten passwords, application access requests, and performance issues caused by existing security solutions.

- 50% of these tickets are deflected by Year 3 due to the adoption of Zero Trust principles (e.g., strong authentication, least-privilege access policies) and the efficiency gains recognized by consolidating under Microsoft’s security stack for endpoint management and identity management.

- Issues not deflected are remediated more quickly than before due to the increased visibility and controls provided by Microsoft security solutions. This allows the help desk to resolve tickets 15% faster.

- The average support ticket takes 30 minutes to resolve between IT and the end user. The average hourly labor costs for an IT admin and end user are $40 per hour; support ticket costs the organization $20 in internal labor costs.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $1.8 million.

Relevant products:

- **Azure AD**
- **Azure AD Conditional Access**
- **Microsoft Sentinel**
- **Microsoft Defender**
- **Microsoft Defender for Endpoint**
- **Microsoft Endpoint Manager**

IT Administration And Help Desk Cost Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Annual help desk calls	B1*8 calls	80,000	80,000	80,000
D2	Percent of calls eliminated due to Microsoft products and the adoption of Zero Trust strategies	Interviews	25%	40%	50%
D3	Annual tickets deflected due to Microsoft products	D1*D2	20,000	32,000	40,000
D4	Reduction in ticket resolution time for remaining tickets	Interviews	15%	15%	15%
D5	Cost per call	Interviews	$20	$20	$20
Dt	IT administration and help desk cost savings	(D3*D5)+(D1*(1-D2)*D4*D5)	$580,000	$784,000	$920,000
	Risk adjustment	↓5%			
Dtr	IT administration and help desk cost savings (risk-adjusted)		$551,000	$744,800	$874,000
	Three-year total: $2,169,800	**Three-year present value: $1,773,095**			

INFRASTRUCTURE MANAGEMENT TIME SAVINGS

Evidence and data. Interviewees said implementing Zero Trust strategies with Microsoft products enhanced their organizations' application development and management practices.

Interviewees said that prior to beginning their Zero Trust journeys, their organizations lacked uniform policies to secure their systems, networks, and infrastructures when developing new applications or onboarding systems from acquisitions. One interviewee said, "Previously, each and every new system was a special unicorn, so no one knew whom to talk to or what order to follow."

Forrester states that "virtualization, microsegmentation, and granular data control strategies are key elements of a Zero Trust strategy. Thanks to their conceptual simplicity, the need to use them is apparent and visible for everyone at the organization." [9]

Zero Trust enabled the interviewees' organizations to standardize processes, eliminating confusion and accelerating deployment and integration speeds.

Interviewees said their organizations were able to:

- **Standardize onboarding, permissions, and access controls.** This reduced the back and forth between infrastructure, security, and business teams and accelerated deployment speeds.
- **Automate routine deployment tasks. Some teams recognized more efficiencies by automatically provisioning and securing new infrastructures.** For example, an enterprise security architect in the energy industry said all of their organization's new deployments are automatically secured through Microsoft Defender for Cloud instead of requiring a security-ticket request.

Relevant products:

- **Azure AD**
- **Azure AD Conditional Access**
- **Microsoft Sentinel**
- **Microsoft Defender for Cloud**
- **Secure Score**
- **Compliance Manager**
- **Azure Networking**
- **Azure Security Center**
- **Microsoft Defender for Endpoint**
- **Microsoft Endpoint Manager**

- **Adopt an infrastructure-as-code methodology to manage security changes through a piece of code approved by their organizations' security teams.** The executive director of information services in the healthcare industry said: "Microsoft has helped us quite a bit around our mergers and acquisitions. They've helped us think about infrastructure as code. They've helped us build out automations to streamline integrating a newly acquired company's technology."
- **Reduce delays previously caused by on-premises infrastructure capacity restraints.** The interviewees explained that their on-premises environments no longer hinder business objectives. The interviewees' organizations can now scale their cloud environments up or down based on their needs instead of undergoing long hardware procurement and deployment cycles.

Interviewees said these changes had a dramatic effect on their organizations.

- The enterprise security architect in the energy industry said it previously took a month to provision new applications but that it now requires just a few hours.
- The executive director of information services in the healthcare industry said onboarding the systems of new acquisitions previously took three to four years but now requires less than one.
- The identity engineer in the manufacturing industry said: “[Using Microsoft security solutions] has allowed us to focus more on our future as opposed to worrying about infrastructure.”

Modeling and assumptions. Forrester assumes the following about the composite organization:

- Previously, new infrastructure provisioning requests could take up to a month to complete. But most of that time was inactive. Requests either sat in a queue or were delayed while business, security, or infrastructure teams clarified a request.
- Previously, the average infrastructure request was for 150 instances. Provisioning and securing one instance took 1.5 FTE hours.
- The composite organization can automate most of the tasks associated with deploying new instances, but IT team members still manually review new deployments to ensure everything is deployed properly. Additionally, unique requests require more manual effort.
- The composite organization acquires one organization during the three-year analysis period. The composite organization is able to completely integrate the acquired company’s systems in one year.

Risks. Forrester recognizes that infrastructure management time savings may vary by organization depending on:

- The frequency of new provisioning requests.
- Existing optimizations around automatically deploying and securing infrastructure.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $1.5 million.

Infrastructure Management Time Savings					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
E1	New Infrastructure requests per year	Composite	24	24	24
E2	Infrastructure and Security FTE hours dedicated per new request	Interviews	225	225	225
E3	Percent reduction in time to deploy and secure new infrastructure due to adopting Zero Trust strategies	Interviews	80%	80%	80%
E4	Average infrastructure and security FTE hourly salary	TEI Standard	$60	$60	$60
E5	Infrastructure deployment time savings	E1*E2*E3*E4	$259,200	$259,200	$259,200
E6	FTEs dedicated to integrating a newly acquired company's systems	Composite	5	5	5
E7	Time savings due to leveraging Microsoft solutions and Zero Trust strategies	Interviews	0%	100%	100%
E8	Average infrastructure FTE salary	TEI Standard	$124,800	$124,800	$124,800
E9	New acquisitions integration savings	E6*E7*E8	$0	$624,000	$624,000
Et	Infrastructure management time savings	E5+E9	$259,200	$883,200	$883,200
	Risk adjustment	↓10%			
Etr	Infrastructure management time savings (risk-adjusted)		$233,280	$794,880	$794,880
	Three-year total: $1,823,040	**Three-year present value: $1,466,203**			

IMPROVED REGULATORY AUDIT AND COMPLIANCE MANAGEMENT

Evidence and data. Data security is an essential component of any organization's security strategy. Now more than ever, organizations are governed by strict data privacy regulations, and noncompliance can result in stiff penalties when violating either government or industry mandates.

- Interviewees said the solutions offered by Microsoft provided their organizations with the visibility and controls they needed to properly secure data and adhere to regulatory requirements.
- The executive director of information services in the healthcare industry said their organization leveraged Microsoft Cloud Access Security Broker (CASB) to gain visibility into its environment from a centralized location. This allowed the organization to protect sensitive data from infiltration or exfiltration.
- Interviewees said Microsoft 365 E5's compliance and data retention tools gave their organizations the ability to retain and easily recall necessary documentation, which greatly improved accuracy and reduced time when conducting audits.
- In a related Forrester study, the director at a manufacturing firm said Microsoft Secure Score reduced the time their organization needed to comply with the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR).[8] Secure Score measures an organization's security posture. The interviewee said: "[Microsoft 365] E5 really enhances our security capabilities. They've helped reduce the cost to perform our twice-yearly security audits by hundreds of thousands of dollars in internal labor and consulting costs."
- Because Zero Trust requirements often exceed many compliance requirements, organizations may find that they already meet a new requirement or need to do relatively little additional work to be compliant.

Relevant products:

- **Azure AD**
- **Azure AD Conditional Access**
- **Microsoft Defender for Cloud Apps**
- **Secure Score**
- **Compliance Manager**
- **Microsoft Defender for Office**
- **Azure Purview**
- **Microsoft Information Protection**
- **Microsoft Endpoint Manager**

Modeling and assumptions. Forrester assumes the following about the composite organization:

- The increased visibility provided by consolidating under Microsoft allows the composite organization to create audit reports much more quickly than before.
- Because Zero Trust strategies often exceed other regulatory requirements, the composite organization needs to perform fewer system-wide changes to adhere to new regulatory requirements.
- FTEs who perform regulatory and compliance audits come from IT, legal, and business teams.
- The average fully burdened salary of an FTE is $120,000.

Risks. Forrester recognizes that improved regulatory audit and compliance management savings may vary by organization depending on:

- The organization’s size.
- The organization’s industry.
- The organization’s geography.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $2 million.

Improved Regulatory Audit And Compliance Management

Ref.	Metric	Source	Year 1	Year 2	Year 3
F1	FTEs dedicated to performing regulatory and compliance audits	Composite	25	25	25
F2	Average audit and compliance FTE salary	TEI Standard	$126,000	$126,000	$126,000
F3	Improved audit and compliance management	Interviews	25%	30%	30%
Ft	Improved regulatory audit and compliance management	F1*F2*F3	$787,500	$945,000	$945,000
	Risk adjustment	↓10%			
Ftr	Improved regulatory audit and compliance management (risk-adjusted)		$708,750	$850,500	$850,500
	Three-year total: $2,409,750		**Three-year present value: $1,986,204**		

IMPROVED IDENTITY AND ACCESS MANAGEMENT

Evidence and data. Interviewees reported that adopting a Zero Trust architecture with Microsoft's solutions led to significant time savings for their organizations' IAM teams. These efficiency gains allowed the teams to focus on value-add initiatives such as improving the organizations' security postures by implementing additional Zero Trust policies and improving user experience (UX). Additionally, IAM team members could be moved to other teams needing additional resources.

The interviewees simplified their IAM environments by consolidating under Azure AD. This eliminated the need to manage on-premises IAM infrastructure and reduced time spent on policy management and vendor management. IAM teams recognized further time savings due to a reduction in application downtime on Azure AD. Lastly, interviewees noted that it was easier and faster to provision/de-provision users.

- The principal architect for technical services in the logistics industry said: "Azure AD has definitely allowed us to become more agile. We can make changes on a dime. Whereas, with our legacy system, product changes were far more cumbersome and painful. … With our previous IAM solution, we often had to write custom code and update our IAM solution across multiple data centers [and] then troubleshoot any problems. With Azure AD, everything is handled by Microsoft. This has allowed us to free up some of our resources and dedicate them to migrating our remaining applications to Azure AD."

- Several interviewees said their organizations had multiple IAM solutions across the cloud and on-premises environments. This substantially increased the complexity of and the effort to manage their environments.

- The identity engineer in the manufacturing industry said: "The MFA that Azure AD has is more user-friendly, and it offers the additional benefits of passwordless sign-in and other modern factors that we leave up to users to choose if they want to use in most instances."

  The same interviewee said the efficiency gains their organization recognized by consolidating its IAM services onto Azure AD, and the reduction in required end-user support will ultimately free up the time of their organization's IAM team requires by 33% to 50%.

- In a related study on Microsoft 365 E5, the CDO of the restaurant chain explained the value Azure AD had on his organization: "Conditional Access has been great for our security team. Managing our users is much easier with Azure Active Directory Premium and Power Apps. We've been able to automate our provisioning and de-provisioning efforts, reducing the burden on our IT team considerably. [Before,] we had around 25 people working only on access management, [with Azure AD], we only have four or five people doing this work. Everyone else is now focused on other security activities."[10]

- Additionally, in a separate study about securing apps with Azure AD, an information security services group professional noted: "It is a lot easier now. We don't have to go provision those services one at a time and create a file share form and things of that nature. When a new hire's account gets rolled out and synced to Azure AD, they get a license automatically assigned and those services are automatically provisioned for us."[11]

Relevant products:

- **Azure AD**
- **Azure AD Conditional Access**

Modeling and assumptions. Forrester assumes the following about the composite organization:

- The average annual salary of a full-time IAM analyst is $120,000.
- The time required to manage IAM systems continues to decrease as the composite organization fully migrates onto Azure AD and progresses through its Zero Trust journey. This reduces the overall number of IAM solutions in the composite organization's environment and IAM teams no longer need to make system upgrades or create and manage custom code.
- The composite's IAM team spends substantially less time provisioning and de-provisioning users by automating these tasks.

Risks. Forrester recognizes that improved identity and access management savings may vary by organization depending on:

- The size of the organization's IAM team before beginning its Zero Trust journey.
- The average salary of the organization's employees.
- The maturity of the organization's Zero Trust journey.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $1.5 million.

Improved Identity And Access Management

Ref.	Metric	Source	Year 1	Year 2	Year 3
G1	FTEs dedicated to managing security environment	Composite	15	15	15
G2	Average security FTE salary	TEI Standard	$120,000	$120,000	$120,000
G3	Reduction in time required to manage security environment due to Microsoft tools	Interviews	25%	40%	50%
Gt	Improved identity and access management	G1*G2*G3	$450,000	$720,000	$900,000
	Risk adjustment	↓10%			
Gtr	Improved identity and access management (risk-adjusted)		$405,000	$648,000	$810,000
	Three-year total: $1,863,000	Three-year present value: $1,512,284			

IMPROVED SECURITY MANAGEMENT

Evidence and data. Interviewees said their organizations were able to optimize multiple tasks with Microsoft's solutions. Interviewees said their organizations gained the ability to apply Zero Trust policies across their environments from a single platform, quickly identify and remediate security concerns, and reduce the complexity of their security environments.

- The security manager at the non-profit explained, "Our Zero trust journey has allowed us to eliminate the technical debt associated with our legacy on-premises security solutions. We've been able to clean house and eliminate the information and operation risk associated with these legacy solutions."
- Interviewees said Azure network security services allowed their organizations to greatly reduce development planning times, integrate security into processes for app development, and adopt infrastructure-as-code methodologies. These benefits greatly improved the efficiency of the organizations' network development efforts.
- Interviewees said Microsoft Sentinel and Microsoft Defender helped security analysts reduce the meant time to resolution (MTTR) for security incidents.
- The solutions architect in the manufacturing industry said: "Migrating to Azure AD and refining our Conditional Access policies has reduced the number of suspicious sign-ins our SOC (security operation center) team needs our help in investigating."
- Interviewees said their organizations' prior solutions had poor alert correlations, which could lead to multiple alerts for a single incident. They also said false positives accounted for upwards of 80% of alerts.
- In a Forrester TEI study for Azure network security services, an enterprise infrastructure architect for a professional services firm explained: "We've been able to shift 320 hours monthly of 'business-as-usual' activities like maintaining and managing systems to 'invest' activities like development of applications and new capabilities." [12]
- By adopting Microsoft Sentinel and Microsoft Defender, the interviewees' organizations were able to reduce the number of false positives they received and better correlate alerts with events.

Relevant products:

- **Azure Security Center**
- **Azure Networking**
- **Microsoft Sentinel**
- **Secure Score**
- **Compliance Manager**
- **Microsoft Defender**
- **Microsoft Endpoint Manager**

Modeling and assumptions. Forrester assumes the following about the composite organization:

- The composite organization dedicates 25 full-time employees to manage its security program.
- In Year 1, the average annual salary of a full-time IAM analyst is $125,000, and salaries increase by approximately 10% each year.
- The time required to manage the security program continues to decrease as the composite's Zero Trust program matures.

Risks. Forrester recognizes that improved security management savings may vary by organization depending on:

- The size of the organization's security team at the beginning of its Zero Trust journey.

- The average salary of the organization's employees.
- Which solutions the organization adopts and their integrations.
- The maturity of the organization's Zero Trust journey.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $3.9 million.

Improved Security Management

Ref.	Metric	Source	Year 1	Year 2	Year 3
H1	FTEs dedicated to managing security environment	Composite	25	25	25
H2	Average security FTE salary	TEI Standard	$125,000	$127,500	$130,050
H3	Reduction in time required to manage security environment due to Microsoft	Interview	50%	55%	60%
Ht	Improved security management	H1*H2*H3	$1,562,500	$1,753,125	$1,950,750
	Risk adjustment	↓10%			
Htr	Improved security management (risk-adjusted)		$1,406,250	$1,577,813	$1,755,675
	Three-year total: $4,739,738		**Three-year present value: $3,901,451**		

REDUCED RISK OF A DATA BREACH

Evidence and data. Interviewees said Microsoft's solution stack offers a robust suite of security solutions that enabled their organizations to progress through their Zero Trust journeys. They said leveraging Microsoft's security solutions enabled their organizations to reduce the risk posed by a variety of security threats such as, phishing, malware, and ransomware attacks. By reducing the likelihood of a compromised account, the organizations reduced the likelihood of a data leak.

Interviewees said that prior to the beginning of their organizations' Zero Trust journeys with Microsoft, they used various point solutions for discrete security tasks. But they said this approach was not only costly and inefficient, but it also limited the visibility that security teams had into their computing environments. Some interviewees said their organizations could not integrate various parts of their legacy infrastructures. Others said legacy infrastructure hindered their organization's ability to progress through its Zero Trust journey. For example, a principal architect in the manufacturing industry said, "Our [legacy IAM solution] prevented us from rolling out MFA to specific regions."

With tools such as Azure Active Directory, Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Microsoft Defender for Identity, and Microsoft Defender for Cloud Apps, the interviewees' organizations now have the correct tools on a single platform to detect and protect against a breach.

Interviewees said the flexibility and interoperability of Microsoft's security solutions made it easier for their organizations to apply Zero Trust principles across their environments. They also said their organizations were able to integrate their remaining point solutions with Microsoft and prioritize the Zero Trust initiatives that were most important to them.

- Interviewees' organizations used Microsoft's security tools to implement Zero Trust strategies, including strong authentication, least-privilege access, and microsegmentation.

- Interviewees said they were better able to detect abnormal user behavior, identify potentially compromised accounts, monitor native and open authentication (OAuth) apps, and detect and remediate attempted malware attacks in real-time.

- The principal architect in the logistics industry said, "[Implementing strong authentication strategies has] allowed us to provide our employees with a better, more secure environment."

- The executive director in the healthcare industry said, "[Using] Zero Trust strategies has made it easier to manage and secure our healthcare systems while also enhancing business processes."

- In a related Forrester study, the CDO of a restaurant chain said their organization

Relevant products:

- **Azure Active Directory**
- **Microsoft Endpoint Manager**
- **Microsoft Defender for Cloud**
- **Microsoft 365 Defender**
- **Microsoft Sentinel**
- **Azure Networking**
- **Azure Security Center**
- **Microsoft Information Protection**

experienced several benefits from using Microsoft 365 E5.[13] They said: “One [benefit] is the ease of identification and increased trust. I have more trust than before because I’m actually capturing more of the incidents. The resolution is much better as well, so the breaches are very limited, and it’s proven to be working very well.”

- In the same study, a director in the manufacturing industry articulated the risk of a security breach for their organization.[14] “We found that we could lose $50 million a year if someone stole some of our proprietary information around some of the products we manufacture. We valued the reduced risk of a security breach due to adopting [Microsoft 365] E5 in the tens of millions of dollars a year, which was enough to justify our investment in E5 by itself.”
- Interviewees said their organizations prioritized securing their employees from phishing, ransomware, and other malware attacks because they were becoming increasingly sophisticated and prevalent, which increased the possibility of a serious data breach. Without tools to protect against these threats, the volume of attacks far exceeded what security teams could handle.

  The executive director of information services in the healthcare industry said: “2021 [was] the year of identity. We feel that this is the new perimeter. Identity has been a strong area of focus, [so] we’ve implemented [Azure AD], added Azure AD Identity Protection, and leveraged AI components to secure our users and data.”
- Interviewees in the manufacturing and logistics industries said implementing the principles of Zero Trust with Microsoft solutions increased their organizations’ Secure Scores by 20 to 30 points since beginning their journeys.

Modeling and assumptions. Forrester assumes the following about the composite organization:

- The average cost of a data breach for the composite organization is $5.04 million.[15]
- The average likelihood that the composite organization has a data breach of 10,000 records or more is 29.6% over two years, or 14.8% per year.[16]
- By deploying Microsoft’s security tools, the composite organization reduces its risk exposure by 50%.

Risks. Data breach avoidance savings may vary by organization depending on:

- The average cost of a data breach for the organization.
- The inherent risk of a data breach.
- The extent to which the organization is able to improve its security posture and capabilities with Microsoft 365 E5.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $780,000.

Reduced Risk Of A Data Breach

Ref.	Metric	Source	Year 1	Year 2	Year 3
I1	Average cost of data breach without Zero Trust	Ponemon Institute	$5,040,000	$5,040,000	$5,040,000
I2	Average cost of data breach with Zero Trust	Ponemon Institute	$4,380,000	$3,710,000	$3,495,000
I3	Difference in average cost of a data breach with Zero Trust	I1-I2	$660,000	$1,330,000	$1,545,000
I4	Average likelihood of data breach	Interviews	14.8%	14.8%	14.8%
I5	Reduced likelihood of a data breach	Interviews	30%	40%	50%
It	Reduced risk of a data breach	I1*I4-I2*(I4*(1-I5))	$292,152	$416,472	$487,290
	Risk adjustment	↓20%			
Itr	Reduced risk of a data breach (risk-adjusted)		$233,722	$333,178	$389,832
	Three-year total: $956,731		**Three-year present value: $780,714**		

UNQUANTIFIED BENEFITS

Additional benefits that customers experienced but were not able to quantify include:

- **Reduced likelihood of regulatory fines.** Improved data security and compliance tools reduced the risk of major data loss events and any resulting compliance fines and legal costs.

- **Improved employee experience.** Nearly all the interviewees said implementing Zero Trust solutions from Microsoft increased employee satisfaction at their organizations. This aligns with Forrester's research that found that very engaged knowledge workers were likely to be satisfied with their technology environments.[17] In comparison, those less engaged were the most dissatisfied with their technology environments.

  Interviewees reported that their legacy security policies and solutions led to high employee burnout. They said the legacy devices were slow, unresponsive, and bogged down by a plethora of security agents. They also said remote workers struggled to be productive with limited access to essential applications and files and due to slowdowns caused by their organizations' VPN solutions.

  Poor device or application performance, difficulty accessing task-critical information, and restrictive security policies are among the top 10 predictors of employee burnout.[18]

  Implementing a Zero Trust architecture helped the interviewees' organizations reduce key causes of employee burnout and increased employee satisfaction. Consolidating under Microsoft's security stack improved device and application performance. Furthermore, Zero Trust architectures empower employees by shifting security responsibility away from users and onto technical controls and by enabling them to work from anywhere.

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Zero Trust solutions from Microsoft and later realize additional uses and business opportunities.

- **Increased business agility.** Implementing a Zero Trust architecture makes an organization inherently more flexible and agile, allowing it to adjust quickly to changing business realities. Since IT spends less time maintaining infrastructure, the department has more bandwidth to support the changing needs of the business.

- **Faster adoption of the newest offerings from Microsoft 365.** Microsoft continuously innovates on existing products, and it creates new products within Microsoft 365 E5. By adopting the E5 solution stack, organizations can take advantage of new offerings more quickly.

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

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
Jtr	Initial planning and implementation	$1,512,500	$0	$0	$0	$1,512,500	$1,512,500
Ktr	Microsoft licensing cost	$0	$1,564,500	$1,827,000	$2,089,500	$5,481,000	$4,502,062
Ltr	Ongoing management costs	$0	$1,892,000	$2,177,120	$2,473,328	$6,542,448	$5,377,521
Mtr	Additional network bandwidth investment	$0	$164,850	$164,850	$164,850	$494,550	$409,958
Ntr	Training costs	$0	$660,000	$99,000	$99,000	$858,000	$756,198
	Total costs (risk-adjusted)	$1,512,500	$4,281,350	$4,267,970	$4,826,678	$14,888,498	$12,558,239

INITIAL PLANNING AND IMPLEMENTATION

Evidence and data. Interviewees said their organizations began their Zero Trust journeys by assessing their existing capabilities. After that, they outlined their desired maturity states and timelines. Their roadmaps spanned each Zero Trust pillar: identities, workloads and infrastructure, endpoints, and data.

Zero Trust identity. Many of the interviewees said their organization's top priority was implementing strong authentication using MFA and SSO. Adopting a cloud-based identity provider, such as Azure AD, is a foundational part of any Zero Trust strategy, enabling organizations to retire their legacy IAM solutions and federating applications. Most of the interviewees' organizations have also begun adopting passwordless authentication methods.

Zero Trust workloads and infrastructure. The interviewees' explained that their organizations secured their workloads by establishing robust cloud governance strategies, inventorying environments, monitoring new and existing workloads, and implementing least-privilege access.

Zero Trust endpoints. The interviewees' organizations secured their devices by adopting modern management solutions, like Microsoft Endpoint Manager (MEM), in order to monitor and enforce device health and compliance for secure access. The interviewees explained that this enabled them to expand access to critical applications and enable BYOD programs.

Zero Trust network. The interviewees adopted network access control solutions to secure their networks. Decision-makers were focused on redrawing their network's perimeters, centralizing network policy management, and automating tasks to reduce complexity and increase visibility. Eliminating the need for a VPN solution was a common first step.

Zero Trust data. Most of the interviewees' organizations are still in the early phases of their Zero Trust data roadmaps. Decision-makers are primarily focused on discovering and classifying data, and they secure their organizations' data by implementing access controls and inspecting data usage patterns.

Modeling and assumptions. Forrester assumes the following about the composite organization:

- The composite organization dedicates 10 internal FTEs to develop its Zero Trust adoption roadmap.
- The composite organization's roadmap prioritizes modernizing its IAM solutions and securing its devices to support hybrid working models. This involves migrating to Azure AD and MEM.
- The composite organization engages with both Microsoft and its partners to implement Azure AD and other key solutions for implementing Zero Trust (e.g., MEM, Microsoft 365 Defender, Azure network security services).

Risks. Initial implementation and planning costs will vary by organization depending on:

- The organization's existing security stack and adherence to Zero Trust strategies.
- The size and scope of the initial deployment.
- The professional services consumed.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.5 million.

Initial Planning And Implementation

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
J1	FTEs involved in implementation Azure AD, Defender, Azure Network Security, Microsoft Endpoint Manager	Composite	10			
J2	Average annual salary	TEI Standard	$125,000			
J3	Percent of time dedicated to implementation	Composite	50%			
J4	Professional services	Interviews	$750,000			
Jt	Initial planning and implementation	(J1*J2*J3)+J4	$1,375,000	$0	$0	$0
	Risk adjustment	↑10%				
Jtr	Initial planning and implementation (risk-adjusted)		$1,512,500	$0	$0	$0
	Three-year total: $1,512,500		**Three-year present value: $1,512,500**			

MICROSOFT LICENSING COST

Evidence and data. The interviewees reported paying both user-based pricing for Microsoft 365 E5 and F3 licenses. The interviewees pay additional consumption-based pricing for Microsoft's solutions not under the Microsoft 365 E5 or F3 licenses.

Modeling and assumptions. Forrester assumes the following about the composite organization:

- Before beginning its Zero Trust journey, half of the composite organization's 5,000 knowledge workers had Microsoft 365 E5 licenses, and half of its 5,000 frontline workers had Microsoft 365 F3 licenses. As a result, the composite organization only needs to purchase licenses for half of its workforce and pay for the consumption of solutions like Microsoft Sentinel, Azure network security services, etc.
- The composite organization's consumption fees increase year over year as it progresses through its Zero Trust journey, leverages additional solutions, and increase its consumption of existing services.

Risks. Licensing costs will vary by organization depending on:

- The number of licenses the organization needs to provide to employees.
- Which Microsoft services the organization consumes.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $4.5 million.

Microsoft Licensing Cost

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
K1	Knowledge workers upgraded to Microsoft 365 E5 licenses	Composite		2,500	2,500	2,500
K2	Incremental Microsoft 365 E5 licensing costs per user per month	Interviews		$25	$25	$25
K3	Incremental Microsoft 365 E5 licensing costs	K1*K2*12 months		$750,000	$750,000	$750,000
K4	Frontline workers given Microsoft 365 licenses	Composite		2,500	2,500	2,500
K5	Microsoft 365 F3 licensing costs per user per month	Interviews		$8	$8	$8
K6	Incremental Microsoft 365 licensing costs for frontline workers	K4*K5		$240,000	$240,000	$240,000
K7	Azure-related costs	Composite		$500,000	$750,000	$1,000,000
Kt	Microsoft licensing cost	K3+K6+K7	$0	$1,490,000	$1,740,000	$1,990,000
	Risk adjustment	↑5%				
Ktr	Microsoft licensing cost (risk-adjusted)		$0	$1,564,500	$1,827,000	$2,089,500
	Three-year total: $5,481,000		**Three-year present value: $4,502,062**			

ONGOING MANAGEMENT COSTS

Evidence and data. Interviewees said that although the ongoing management of Microsoft's security solutions is significantly less labor-intensive than their legacy solutions, their organizations still require administrative support.

Additionally, the interviewees' organizations are still in the early phases of their Zero Trust journeys, so they are still implementing a wide range of Zero Trust strategies. Decision-makers are also focused on improving efficiency by improving visibility across their organizations' digital environments and automating tasks whenever possible.

Modeling and assumptions. Forrester assumes the following about the composite organization:

- The composite organization dedicates six IT FTEs to the ongoing management of Zero Trust solutions from Microsoft in Year 1.
- The FTEs work with Microsoft and a Microsoft partner to implement Zero Trust strategies in the organization's roadmap. This involves continuing to implement passwordless authentication, migrating applications to Azure AD, securing the organization's data, and finding new opportunities for automation.

Risks. Ongoing management costs will vary depending on:

- The organization's number of users and locations.
- The solutions in use and slated for adoption at the organization.
- Whether or not the organization needs professional services.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $5.4 million.

Ongoing Management Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
L1	IT FTEs dedicated to ongoing management	Composite		6	8	10
L2	Average IT FTE salary	TEI Standard		$120,000	$122,400	$124,848
L3	Ongoing professional services	Interviews		$1,000,000	$1,000,000	$1,000,000
Lt	Ongoing management costs	L1*L2+L3	$0	$1,720,000	$1,979,200	$2,248,480
	Risk adjustment	↑10%				
Ltr	Ongoing management costs (risk-adjusted)		$0	$1,892,000	$2,177,120	$2,473,328
	Three-year total: $6,542,448			**Three-year present value: $5,377,521**		

ADDITIONAL NETWORK BANDWIDTH INVESTMENT

Evidence and data. Some interviewees said their organizations required additional bandwidth to support additional network traffic resulting from increasing their cloud environments. This increased the number of frontline workers who required access to the organization's applications and created additional network demands on solutions from Microsoft.

Risks. Additional bandwidth investment costs may vary by organization depending on:

- The organization's existing bandwidth.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $410,000.

Additional Network Bandwidth Investment

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
M1	Additional network bandwidth investment	Interviews		$157,000	$157,000	$157,000
Mt	Additional network bandwidth investment	M1		$157,000	$157,000	$157,000
	Risk adjustment	↑5%				
Mtr	Additional network bandwidth investment (risk-adjusted)		$0	$164,850	$164,850	$164,850
	Three-year total: $494,550		**Three-year present value: $409,958**			

TRAINING COSTS

Evidence and data. Interviewees said that conducting internal training sessions for Microsoft solutions caused workflow changes at their organizations. These sessions encompassed any number of topics, including enabling MFA and passwordless authentication and using new workflows to request infrastructure.

Interviewees reported that training requirements were fairly minimal and that training often consisted of short workshops or lunch-and-learn sessions. They also said their organizations integrated training sessions into the onboarding processes for new hires.

Modeling and assumptions. Forrester assumes the following about the composite organization:

- The composite incurs internal labor costs associated with training its entire workforce.
- The composite organization trains its entire workforce in Year 1. After that, it only trains newly hired employees.
- The composite organization experiences 15% employee churn each year.

Risks. The internal labor costs associated with training employees will vary by organization depending on:

- How familiar the organization's workforce is with Zero Trust.
- The average fully burdened salary of the organization's workforce.

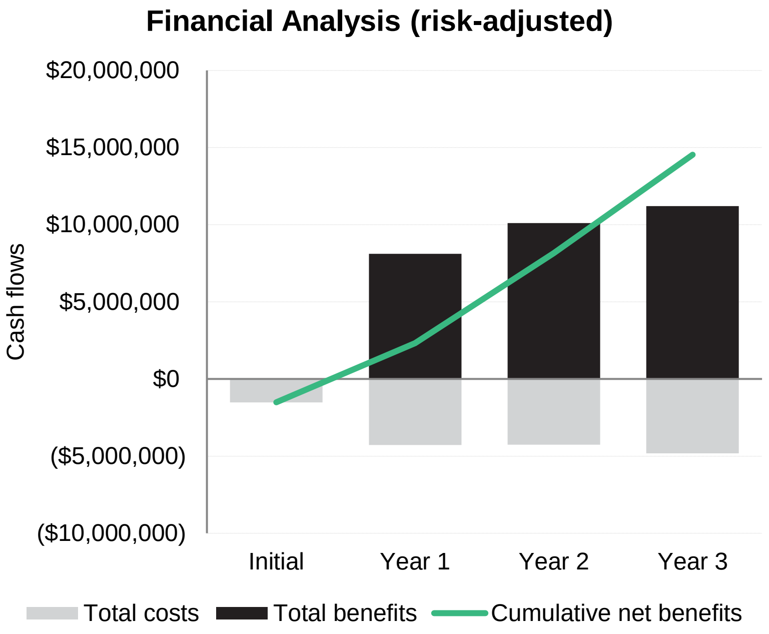
Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $760,000.

Training Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
N1	Employees trained on Zero Trust features for the first time	Assumption		10,000	1,500	1,500
N2	Average training time dedicated to training employees for the first time (hours)	Interviews		2	2	2
N3	Average fully burdened FTE salary	TEI Standard		$30	$30	$30
Nt	Training costs	N1*N2*N3	$0	$600,000	$90,000	$90,000
	Risk adjustment	↑10%				
Ntr	Training Costs (risk-adjusted)		$0	$660,000	$99,000	$99,000
	Three-year total: $858,000		**Three-year present value: $756,198**			

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS



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	($1,512,500)	($4,281,350)	($4,267,970)	($4,826,678)	($14,888,498)	($12,558,239)
Total benefits	$0	$8,111,250	$10,107,135	$11,205,301	$29,423,686	$24,145,575
Net benefits	($1,512,500)	$3,829,900	$5,839,165	$6,378,623	$14,535,188	$11,587,336
ROI						92%
Payback						<6 months

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: 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: "The Total Economic Impact™ Of Microsoft Azure Sentinel," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, November 2020.

[3] Source: "The Total Economic Impact™ Of Microsoft 365 Enterprise E5," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, December 2020.

[4] Source: "Cost of a Data Breach Report 2021," Ponemon Institute, July 2021.

[5] Source: "Enhance EX With Zero Trust," Forrester Research, Inc., July 13, 2020.

[6] Source: "The Total Economic Impact™ Of Microsoft 365 Enterprise E5," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, December 2020.

[7] Ibid.

[8] Ibid.

[9] Source: "The Zero Trust eXtended (ZTX) Ecosystem," Forrester Research, Inc., August 23, 2021.

[10] Source: "The Total Economic Impact™ Of Microsoft 365 Enterprise E5," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, December 2020.

[11] Source: "The Total Economic Impact™ Of Securing Apps with Microsoft Azure Active Directory," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, August 2020.

[12] Source: "The Total Economic Impact™ Of Microsoft Azure Network Security," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, October 2021.

[13] Source: "The Total Economic Impact™ Of Microsoft 365 Enterprise E5," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, December 2020.

[14] Ibid.

[15] Source: "Cost of a Data Breach Report 2021," Ponemon Institute, July 2021.

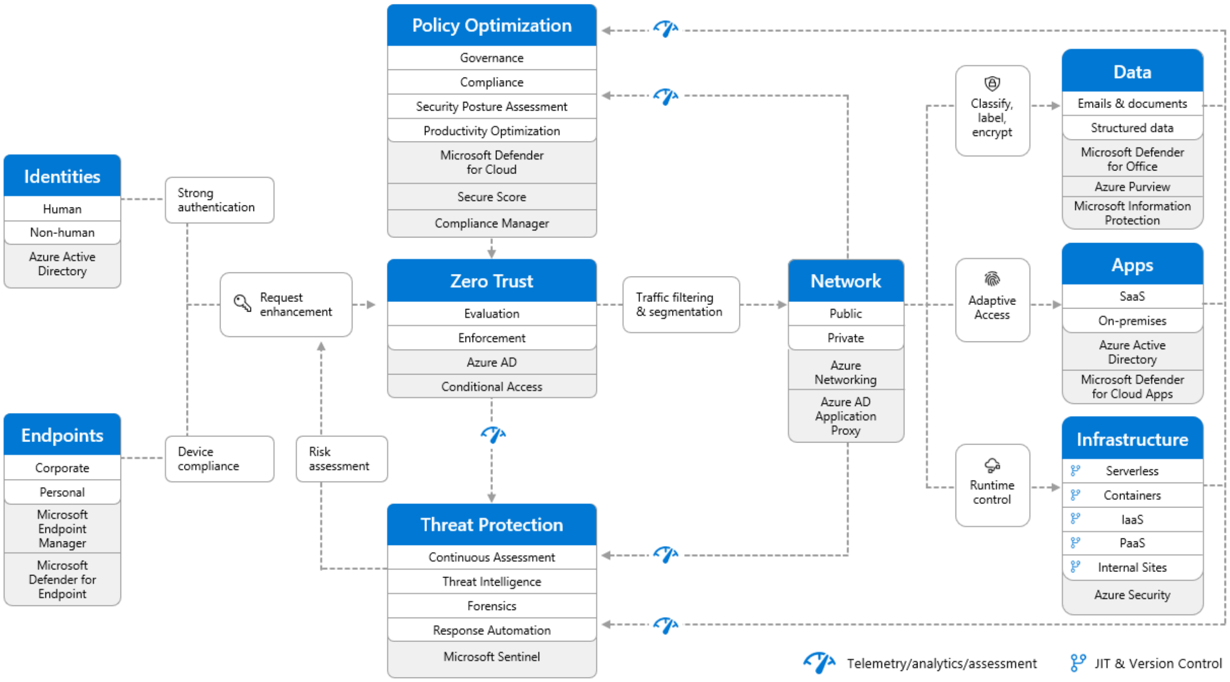
[16] Source: "Cost of a Data Breach Report 2019," Ponemon Institute, July 2019.

[17] Source: Forrester Analytics Global Business Technographics® Workforce Benchmark Survey, 2019.

[18] Ibid.

Adopting a Zero Trust architecture with Microsoft

Microsoft offers a comprehensive portfolio of security solutions which enable every organization to implement an end-to-end Zero Trust strategy.



A Zero Trust security model serves as a comprehensive cybersecurity strategy that extends across the entire digital estate—inclusive of identities, endpoints, network, data, apps, and infrastructure.

The foundation of Zero Trust security is **Identities**. Both human and non-human identities need strong authorization, connecting from either personal or corporate **Endpoints** with a compliant device.

As a unified policy enforcement, the **Zero Trust Policy** intercepts the request, and explicitly verifies signals from all six foundational elements based on policy configuration and enforces least privileged access. In additional to telemetry and state information, the risk assessment from threat protection feeds into the policy engine to automatically respond to threats in real-time. Policy is enforced at the time of access and continuously evaluated throughout the session.

The telemetry and analytics feeds into the **Threat Protection** system. The risk assessment feeds into the policy engine for real-time automated threat protection, and additional manual investigation if needed.

Traffic filtering and segmentation is applied to the evaluation and enforcement from the Zero Trust policy before access is granted to any public or private **Network**. **Data** classification, labeling, and encryption should be applied to emails, documents, and structured data. Access to **Apps** should be adaptive, whether SaaS or on-premises. Runtime control is applied to **Infrastructure**, with serverless, containers, IaaS, PaaS, and internal sites, with just-in-time (JIT) and Version Controls actively engaged.

Finally, telemetry, analytics, and assessment from the Network, Data, Apps, and Infrastructure are fed back into the Policy Optimization and Threat Protection systems.

To learn more about how Microsoft can help enable your Zero Trust strategy, visit aka.ms/zerotrust

FORRESTER®