

A Forrester Total Economic Impact™  
Study Commissioned By Microsoft  
May 2020

# The Total Economic Impact™ Of Microsoft Cloud App Security

Cost Savings And Business Benefits  
Enabled By Microsoft's Cloud App  
Security Broker

# Table Of Contents

|  |           |
|--|-----------|
| <b>Executive Summary</b>   | <b>1</b>  |
| Key Findings   | 1         |
| TEI Framework And Methodology  | 3         |
| <b>The Cloud App Security Customer Journey</b>                           | <b>4</b>  |
| Interviewed Organizations  | 4         |
| Key Challenges In Market That CASBs Address                              | 4         |
| Solution Requirements By Market  | 6         |
| Key Results Offered By Microsoft's CASB                                  | 6         |
| Composite Organization   | 9         |
| <b>Analysis Of Benefits</b>  | <b>10</b> |
| Decreased Effort To Assess And Provide Visibility Into Security And Risk | 10        |
| Lowered Time And Effort To Remediate Incidents                           | 11        |
| Improved Ability To Avoid Data Breach                                    | 13        |
| Improved Compliance And Audit Reporting                                  | 14        |
| Optimized Resources  | 15        |
| Flexibility  | 16        |
| <b>Analysis Of Costs</b>   | <b>17</b> |
| Licensing Costs  | 17        |
| Implementation And Ongoing Management                                    | 17        |
| <b>Financial Summary</b>   | <b>19</b> |
| <b>Microsoft Cloud App Security: Overview</b>                            | <b>20</b> |
| <b>Appendix A: Total Economic Impact</b>                                 | <b>21</b> |

**Project Director:**  
Adrienne Capaldo  
**Project Contributor:**  
Sam Sexton

## ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit [forrester.com/consulting](https://forrester.com/consulting).

© 2020, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to [forrester.com](https://forrester.com).

# Executive Summary

## Key Benefits



Reduction in time and effort to remediate incidents:

**80%**



Threats automatically eliminated by MCAS with automated processes like policy setting:

**75%**



Reduced the likelihood of a data breach by:

**40%**

Microsoft provides its Cloud App Security solution (MCAS), which is a cloud access security broker (CASB). CASBs are cloud-based security solutions that help organizations protect their cloud applications against a variety of cyberthreats. Cloud App Security provides organizations with visibility into and control over their cloud apps, services, and data, and it identifies, detects, and addresses cybersecurity threats. Microsoft commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Cloud App Security. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Cloud App Security on their organizations. Forrester utilizes conservative estimates throughout the study to present potential return on investment, and it is important to note that organizations may have significantly higher outcomes based on their Cloud App Security usage.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four customers with years of experience using Cloud App Security. Prior to using Cloud App Security, the customers tried to address vulnerabilities with more conventional security suites. However, prior attempts yielded limited success and left customers with low visibility into their data, user behavior, and sensitive data moving onto the cloud. These limitations led to the rise of shadow IT, difficulty recognizing and remediating security threats, and the need to rapidly adapt to new compliance requirements for the cloud. With Cloud App Security, organizations were able to gain visibility across all their native and third-party applications, allowing them to more easily monitor the security and risks associated with their cloud applications and sensitive data. It also improved their ability to detect and remediate incidents, improved compliance, and improved the overall ease of management of their cloud application portfolios. Microsoft aligns these benefits into four key pillars: identity and access management, threat protection, information protection, and cloud security posture management.

## Key Findings

**Quantified benefits.** The following risk-adjusted present value (PV) quantified benefits are representative of those experienced by the interviewed companies:

- › **Led to 80% reduction in time to monitor, assess, and govern cloud application portfolio risks.** As the threat landscape changes and evolves, the amount of time required to monitor cloud apps, data security, and risks rises precipitously each year. Without Cloud App Security, this was a daunting task that would take SecOps teams a significant amount of time. The visibility Cloud App Security provides significantly reduces the amount of time and effort required to monitor environments and assess the risk of discovered applications, which strengthens the composite organization's cloud security posture. Interviewees told Forrester they were able to reduce time in monitoring, assessment, and governance of cloud risk by 80% by Year 3. Over three years, the time savings are worth more than \$571,000.
- › **Dramatically lowered the time and effort to remediate incidents.** The composite organization faces thousands of security incidents yearly, and that number increases as more end points are added and threats evolve



**ROI**  
**151%**



**Benefits PV**  
**\$8.89 million**



**NPV**  
**\$5.35 million**



**Payback**  
**<3 months**

and become harder to manage. With Cloud App Security, organizations are better able to protect against threats and safeguard their information, wherever it may be located. Forrester found that Cloud App Security automatically eliminates 75% of threats due to its increased visibility and automation capabilities. That leaves just 25% of threats for SecOps staff members to identify and remediate on their own. With Cloud App Security, the organizations were able to reduce the time to discover and remediate incidents by 80%. This also substantially reduced the need for IT help desk support, saving time for both end users and various IT staff members. Over three years, the savings are worth more than \$6 million.

- › **Reduced the likelihood of a data breach by 40%.** The increased visibility and tools available to organizations after implementing Cloud App Security provide stronger security, even as the organization scales to cover more sensitive data assets. In fact, the reduction in likelihood decreases further. Utilizing Cloud App Security, organizations guard against security threats, better protect their data, ensure and authorize correct user access, and reduce the likelihood of a security breach to less than 1%. This saves more than \$1.6 million over three years.
- › **Kept compliance costs down by reducing time spent on audit reporting by 90%.** Moving to the cloud opens organizations up to new regulatory and client requirements for security. Cloud App Security provides improved visibility and detailed audit trails that make it much easier to find and compile details required for audit requests, such as who has accessed what information and data. With Cloud App Security, organizations can prepare for audits in 10% of the time they would have needed without Cloud App Security, saving significant time for SecOps, IT, and internal auditing personnel. This accumulates to a savings of nearly \$100,000 over three years.
- › **Made more efficient future hires due to automatic and policy-setting features, saving more than \$110,000 over three years.** The ability to set policies, automatically configure settings, and improve visibility reduces the overall amount of time required manage existing cloud application portfolios. That allows staff to monitor, assess, and govern even as threats and cloud application environments grow every year. As a result of the improvement in cloud security posture management, the organizations are able to avoid hiring SecOps personnel to cover the work of 0.5 FTEs each year and can instead hire more efficiently for other tasks.

**Costs.** The interviewed organizations experienced the following risk-adjusted PV costs:

- › **Licensing costs of \$1.26 million each year.** Cloud App Security charges a per-user licensing fee of \$3.50 per month. While the fee stays the same over three years, the number of employees increases.
- › **Implementation and ongoing management of \$99,000 over three years.** After a relatively simple initial deployment that requires 15 person-hours of work, Cloud App Security requires only 12 person-hours per week to manage and maintain.

Forrester's interviews with four existing customers and subsequent financial analysis found that an organization based on these interviewed organizations experienced benefits of \$8.89 million over three years versus costs of \$3.54 million, adding up to a net present value (NPV) of \$5.35 million and an ROI of 151%.

The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

## TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing Microsoft Cloud App Security.

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 Cloud App Security can have on an organization:



### **DUE DILIGENCE**

Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to Cloud App Security.



### **CUSTOMER INTERVIEWS**

Interviewed four organizations using Cloud App Security to obtain data with respect to costs, benefits, and risks.



### **COMPOSITE ORGANIZATION**

Designed a composite organization based on characteristics of the interviewed 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 interviewed organizations.



### **CASE STUDY**

Employed four fundamental elements of TEI in modeling Microsoft Cloud App Security's impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide 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 report to determine the appropriateness of an investment in Microsoft Cloud App Security.

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 Cloud App Security Customer Journey

## BEFORE AND AFTER THE CLOUD APP SECURITY INVESTMENT

### Interviewed Organizations

For this study, Forrester conducted four interviews with Microsoft Cloud App Security customers. Interviewed customers include the following:

| INDUSTRY                    | REGION  | INTERVIEWEE           | NUMBER OF ENDPOINTS PROTECTED | NUMBER OF EMPLOYEES |
|-----------------------------|---|-----------------------|-------------------------------|---------------------|
| Manufacturing               | Global operations, headquartered in Australia     | Cybersecurity analyst | 13,000                        | 20,000              |
| University and health care  | Headquartered in North America                    | Cloud operations lead | 60,000                        | 60,000              |
| Health care                 | Headquartered in North America                    | CIO                   | 7,000                         | 17,000              |
| Medical device manufacturer | Global operations, headquartered in North America | Technical manager     | 50,000                        | 132,000             |

For the companies interviewed, two moved from a previous CASB to Cloud App Security, and two deployed Cloud App Security as their first CASB.

### Key Challenges In Market That CASBs Address

Interviewees shared several challenges they faced that led them to implement Microsoft Cloud App Security:

- › **Limited visibility led to a lack of understanding of existing cloud application portfolios.** As the interviewed organizations increased their reliance on and access to cloud applications prior to using a CASB, they found that they had frustratingly limited visibility into which applications users accessed, what corporate data was being accessed and stored in cloud applications, and how the data was being used. The technical manager at the medical device manufacturer stated: “We had absolutely no real visibility into the environment. The only visibility we really had in detail was some mail. But when it came to the other cloud services that we focused on, we had no visibility.” Prior to investing in Cloud App Security, the interviewees were either not using any type of security solutions for their cloud applications or they had multiple solutions that did not provide the visibility and clarity they needed to properly understand and assess the risk of their cloud application portfolios.

“Previously, we had a knowledge gap. We didn’t realize we could take all these different cloud services we had — which is a lot — and get that single pane of glass to really get control of our applications.”

*Cloud operations lead, university and health care*



› **Shadow IT specifically created a large concern.** Interviewees were shocked to learn about the number of cloud applications their end users were accessing. Nearly every interviewee said that members of their organizations were using more than 5,000 applications — from corporate cloud applications to consumer-facing cloud applications. The technical manager at the medical device manufacturer said, “We discovered close to 9,000 applications that people are accessing.” With limited visibility, the organizations were unable to identify which applications were being used across their organizations. The cybersecurity analyst at the manufacturing organization said: “Previously, we had no visibility into shadow IT. I couldn’t see my applications, and I had no control over them.” And even more concerning, with this limited visibility into shadow IT, the organizations could not accurately understand the risks and compliance of their cloud apps and the data assets they held.

› **With the move to the cloud, organizations faced new security and compliance requirements.** The need to move to the cloud required moving sensitive information off-premises, which also required new security measures to make sure the data assets were protected. Additionally, many interviewees also had to worry about compliance and adhering to rules that govern sensitive data on the cloud. Often, an enterprise can only move its workloads and data to the cloud if it checks the box and uses a CASB. The CIO from the health care organization said: “We’ve been somewhat slow to move to the cloud because of protected health information (PHI) and Health Insurance Portability and Accountability Act (HIPAA) regulations. But as we started to research CASBs, we realized we can get good governance, compliance, and audit support as we move towards the cloud — whether it’s software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), or platform-as-a-service (PaaS).” Without a CASB in place, organizations struggled to ensure the apps their end users accessed met security policies and compliance requirements. One interviewee said: “We never had anybody who was reviewing what was being set up, how that should be approved, what it could access, and who could access it. You could basically create anything you wanted and give it any type of permissions. It was scary.” With the lack of visibility into sensitive data being shared within and across apps, organizations strove to guarantee their compliance regulations were being met.

“We discovered close to 9,000 applications that people are accessing, and we want to shut down close to 1,600 applications.”

*Technical manager, medical device manufacturer*



“When we began looking at CASBs, we knew that our HIPAA policies and procedures that are part of our on-premises cybersecurity framework had to be incorporated into our CASB framework as well. We wanted visibility into who is using and accessing that data.”

*CIO, health care*



- › **When security threats occurred, organizations often struggled to recognize and remediate the issues.** Due to either myriad disparate tools or a lack of a CASB solution altogether, interviewees faced multiple issues detecting threats and protecting against them. The lack of visibility meant they often faced long dwell times, and they were unable to be proactive against threats. They were only reactive. The cybersecurity analyst for the manufacturing organization said, “Before Cloud App Security, sometimes we could not even detect an issue — maybe not until someone noted that something was wrong.” The organizations struggled to understand where issues began, they lacked the automated tools to help them identify and investigate threats, and they were unable to easily monitor users and their activities. All of this led to SecOps and IT staff members “running around with their heads on fire” as they worked to assess and protect their cloud application environments. One interviewee said: “Without Cloud App Security, we struggled to know who was compromised. We would have to try to retrace everything someone did manually in some sort of local log. It wasn’t very efficient. We’d waste a couple of hours in an effort just to get up and looking at the logs.” Without a CASB solution, detecting and protecting against threats was challenging.

“Everything prior to MCAS was very much reactive. We’d see these big phishing attacks, but we’d only see them after the fact. We wouldn’t have any type of alerting. To understand what happened, we’d have to go and look at logs manually. A lot of times, there’d be all these different panes of glass. So, consolidating that visibility into MCAS was obviously huge for our organization.”

*Cloud operations lead, university and health care*



## Solution Requirements By Market

The interviewed organizations searched for a solution that could:

- › Provide visibility into the cloud apps being used across their organizations and how the data in those apps was accessed.
- › Provide easy deployment and low implementation requirements, a low learning curve, and integrate well with existing applications, regardless of vendor.
- › Help them gain a true understanding of their existing risks and compliance concerns across their cloud applications.
- › Support them in enforcing compliance standards across these applications.
- › Help the SecOps and IT teams detect and protect against security threats, such as comprised users or malware in their cloud apps.

After extensive RFPs and business case processes evaluating multiple vendors, the interviewed organizations chose Microsoft Cloud App Security.

## Key Results Offered By Microsoft’s CASB

The interviews revealed the following key results from the Microsoft Cloud App Security investment:

“Previously, I had maybe up to five different security tools that I needed to monitor individually and on a daily basis to check what was going on. But now, with MCAS, I can see everything together — all events in one place and connected. It’s greatly decreased my time to get that visibility.”

*Cybersecurity analyst, manufacturing*





- › **Companies gained visibility across their entire cloud application portfolio through a single pane of glass.** By implementing Cloud App Security, the interviewed organizations were able to discover all the cloud apps being accessed and understand the data that was contained within the apps and how that data was being accessed and shared. That allowed them to truly understand their cloud security postures. The organizations benefited from Cloud App Security ensuring coverage across all the various types of cloud apps their end users accessed with integrations, Microsoft-native solutions, and third-party solutions. The CIO of the health care organization said: “We know exactly what’s out there. . . . We are able to see and understand how our data might move between different applications.” This visibility also allowed organizations to get a true understanding of their shadow IT, including the number of applications end users were utilizing. They were also able to assess which applications they would like to be sanctioned versus unsanctioned. The technical manager of the medical device manufacturer said, “We’re in the process now of understanding these 9,000 applications we discovered with Cloud App Security, and we found at least 1,600 applications we want to shut down.” SecOps and IT can now easily understand their cloud application portfolios with an easy-to-use dashboard that automatically pulls together this data.
- › **Organizations benefited from how Cloud App Security integrated with their existing architectures.** Interviewees said Cloud App Security gave their organizations the flexibility to integrate with their existing architectures, including log ingestion from firewalls, secure web gateways and security information and event management solutions (SIEMs), API-based connectors, and reverse-proxy integration with their primary identity and access management (IAM) providers. The cloud operations lead at the university and health care organization told Forrester: “With the cloud discovery feature, we were able to pull all our firewall data and get visibility into all our applications, including the ones we API-connected through Microsoft. Cloud App Security helps us decide if certain applications are risky, and we can apply policies against them.” Cloud App Security created a single management experience for the interviewed organizations that provided them with the visibility they needed to truly understand where threats may exist and what policies and sanctions they may need to put in place. This safeguards the organizations, protects their data and those who access it, and ensures they can strengthen their cloud security postures.

“Another useful feature of MCAS is open authentication of apps. Previously, it was really hard to identify how our users shared information with the third-party applications.”

*Cybersecurity analyst,  
manufacturing*



› **Cloud App Security helped interviewees create governance and policies to enforce security and compliance needs more easily, reducing the effort to assess risks and provide security.** The interviewees said Cloud App Security helped their organizations understand what data is out there, where sensitive data exists, and how it moves across their organizations. It also helped them enforce compliance through automated alerts and suggested remediation actions. After Cloud App Security helped the organizations discover the cloud applications their users were accessing, they were able to use Cloud App Security to apply governance where necessary to control access and use of the apps. Cloud App Security provided these organizations with the ability to easily create policies based on evaluated behavior of cloud apps and how users were accessing data, and it allowed the organizations to continuously monitor and automatically detect risky applications. This strengthened their cloud security postures. The cloud operations lead for the university and health care organization said, “After we discover the apps, Cloud App Security tells us if an app is deemed risky, and we can write policy and automate future alerts if something similar happens.” Cloud App Security also helped the organizations protect their sensitive data by enforcing controls and policies based on the sensitivity of that data. Finally, Cloud App Security enabled the organizations to implement policies that alert SecOps to potential data leakage, enforce DLP and compliance policies, flag policy violations, and automatically apply restrictions if needed. Cloud App Security made governance simpler and ensured the organizations were easily able to meet compliance and auditing requests due to the visibility their centralized dashboards provided.

› **Companies more easily detected and remediated security threats.** Cloud App Security provided the interviewed organizations with better analytics, alerts, and automated processes that improved their abilities to detect, investigate, and remediate security threats in their cloud application environments. Cloud App Security alerts them to anomalies or suspicious behavior in compromised user accounts, internal threats like mass downloads or unusual activities, and potential malware breaches. With Cloud App Security, organizations can closely monitor a variety of activities, receive investigation priority, and obtain suggestions to quickly remediate threats. The CIO of the health care organization said, “Working with Microsoft . . . really helped us. If we have a threat, we can identify it so we can defend [against it], protect [our organization], and respond and recover quickly.” With increased visibility, Cloud App Security eliminates time-consuming investigation from the remediation process, and it quickly provides the information that organizations need to protect themselves.

The combination of these results allowed existing SecOps and IT teams could more easily, with reduced time and effort and improved quality, support and protect their cloud application environment.

“[Data loss prevention] is important to us. Because we have specific compliance standards like HIPAA, we created and enforced policies and alerts to protect our apps and data, and to ensure compliance.”

*Cloud operations lead, university and health care*



“Our mean-time-to-detect and mean-time-to-remediate are much improved since we implemented MCAS. Previously, it was super manual, and it could take days or weeks. Now, we are alerted and can jump in.”

*Technical manager, medical device manufacturer*



## Composite Organization

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an associated ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four companies that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization that Forrester synthesized from the customer interviews has the following characteristics:

**Description of composite.** The composite organization is a global organization with most of its operations based in North America and 30,000 employees.

**Deployment characteristics.** Prior to deploying Cloud App Security, the composite organization did not have CASB capabilities. The composite organization purchased Cloud App Security to protect each of its end points. As the organization grows, it continues to add Cloud App Security to each new end point. The security operations team manages Cloud App Security with two employees supporting it as the main part of their overall job duties.



### Key data points about composite organization

- Global manufacturing organization
- 30,000 employees' endpoints protected in Year 1
-

# Analysis Of Benefits

## QUANTIFIED BENEFIT DATA AS APPLIED TO THE COMPOSITE

| Total Benefits     |  |             |             |             |              |               |
|--------------------|--|-------------|-------------|-------------|--------------|---------------|
| REFERENCE (TOTALS) | BENEFIT  | YEAR 1      | YEAR 2      | YEAR 3      | TOTAL        | PRESENT VALUE |
| Atr                | Decreased effort to assess and provide visibility into security and risk | \$164,268   | \$234,234   | \$304,200   | \$702,702    | \$571,466     |
| Btr                | Lowered time and effort to remediate incidents                           | \$1,694,475 | \$2,507,080 | \$3,722,524 | \$7,924,079  | \$6,409,186   |
| Ctr                | Improved ability to avoid data breach                                    | \$669,375   | \$683,719   | \$694,238   | \$2,047,331  | \$1,695,170   |
| Dtr                | Improved compliance and audit reporting                                  | \$39,462    | \$39,462    | \$39,462    | \$118,385    | \$98,135      |
| Etr                | Optimized resources  | \$0         | \$64,125    | \$64,125    | \$128,250    | \$111,291     |
|                    | Total benefits (risk-adjusted)   | \$2,567,580 | \$3,528,619 | \$4,824,548 | \$10,920,746 | \$8,885,248   |

### Decreased Effort To Assess And Provide Visibility Into Security And Risk

Prior to investing in Cloud App Security, the interviewed organizations suffered due to limited visibility into their cloud application portfolios. They either did not have a CASB in place or they had multiple data security and data loss prevention (DLP) solutions and needed to piece together information from these various solutions. This lack of visibility created issues around shadow IT, as the organizations did not have real insights into which applications were being used, how data was moving around the organizations, and what sensitive data was being accessed by whom.

Through the implementation of Cloud App Security, the organizations greatly decreased the effort required to assess and protect their cloud application portfolios. With integrations across Microsoft-native solutions and third-party applications, Cloud App Security enabled them to truly understand which applications their colleagues were accessing, in an easy-to-use dashboard that provided a single pane of glass by which to manage the cloud application portfolio. Cloud App Security enabled these orgs to assess the risks associated with these apps, which allowed teams to decide which applications required more governance. Finally, Cloud App Security enabled the organizations to truly understand their sensitive data. If anything was at risk for exposure, Cloud App Security helped them take steps to address these issues through a single management platform. With Cloud App Security, the organizations are able to greatly reduce the SecOps labor hours allocated to monitoring cloud apps, data security, and risk while strengthening its cloud security posture.

For the composite organization, Forrester assumes that:

- › Prior to the investment in Cloud App Security, SecOps spent 90 person-hours per week monitoring the security and risk posture of cloud applications.

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of more than \$8.8 million.



**80% reduction in time to monitor, assess, and govern cloud application portfolio risk**

› With Cloud App Security, the organization initially reduces time spent on monitoring, assessing, and governing cloud risk by 60%. As it becomes more comfortable with Cloud App Security and improves how it uses the solution and becomes more proactive with it, this increases to 80% by Year 3.

› An average fully loaded salary for a SecOp FTE is \$65 per hour.

It is important to note that these numbers and estimates may vary from organization to organization, and that the value of this benefit may create higher outcomes based on an organization’s Cloud App Security usage.

The decreased effort to assess and provide visibility into security and risk can vary with:

- › The number of hours spent per week on these tasks prior to the investment in Cloud App Security.
- › How adept SecOps is at using Cloud App Security to monitor, assess, and govern the cloud environment.
- › The salary of SecOps personnel.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a conservative three-year risk-adjusted total PV of \$571,466.

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

**Decreased Effort To Assess And Provide Security And Risk Visibility: Calculation Table**

| REF. | METRIC   | CALCULATION  | YEAR 1    | YEAR 2    | YEAR 3    |
|------|--|--|-----------|-----------|-----------|
| A1   | SecOps labor hours allocated to monitor cloud apps, data security, and risk prior to MCAS          | 90 hours * 52 weeks per year in Year 1 (increases YoY)                                   | 4,680     | 5,720     | 6,500     |
| A2   | Reduction in time to monitor, assess, and govern cloud risk post-adoption of MCAS, as a percentage | Interview finding  | 60%       | 70%       | 80%       |
| A3   | SecOps hourly salary   | (\$100,000 * 1.35X benefits modifier)/2,080 working hours per year (rounded value shown) | \$65      | \$65      | \$65      |
| At   | Decreased effort to assess and provide security and risk visibility                                | A1*A2*A3   | \$182,520 | \$260,260 | \$338,000 |
|      | Risk adjustment  | ↓10%   |           |           |           |
| Atr  | Decreased effort to assess and provide security and risk visibility (risk-adjusted)                |  | \$164,268 | \$234,234 | \$304,200 |

**Lowered Time And Effort To Remediate Incidents**

The interviewed organizations previously struggled to gain the visibility required to detect and protect against threats. Prior to investing in Cloud App Security, they were often in a reactive stance and without the proper visibility to proactively detect compromised user or admin accounts, identify threats from within, or detect malware in their cloud application portfolios.

With Cloud App Security, the organizations were able to better detect, investigate, and remediate security incidents and protect their information — wherever it may be located — with access to Cloud App Security analytics, alerts, and automated processes. They were also able to proactively create policies to automatically protect against certain scenarios, such as revoking access of a compromised account. With Cloud App Security, they were able to have a detailed audit trail to truly understand how an incident occurred and be able to better trace and



**75%**  
Threats automatically eliminated with MCAS due to automated processes

investigate the issue. They also received suggestions for investigation prioritization to ensure they focused on top areas of concern. The organizations said this helped IT and end users reduce the time they spent involved in an incident, which reduced help desk call time. The increased visibility that Cloud App Security provides eliminated time-consuming investigation from the remediation process and provided the information needed to protect the organizations quickly.

For the composite organization, Forrester assumes that:

- › Initially, it protects 30,000 employee's end points. This grows at a rate of 10% year-over-year.
- › Across these devices, it is assumed that 2,000 incidents will occur in Year 1. However, as the threat landscape continues to evolve and more intelligent attacks occur, this number increases each year.
- › With automated processes like policies put in place, Cloud App Security automatically eliminates 75% of the threats coming into the organization.
- › Prior to investing in Cloud App Security, the organization spent an average of 96 person-hours to discover and remediate cloud-based incidents.
- › With Cloud App Security, the organization initially reduces the time to discover and remediate incidents by 60%. As the SecOps team improves how it uses Cloud App Security to detect and protect against cybersecurity threats, this increases to 80% by Year 3.
- › Additionally, the model looks at how Cloud App Security helps reduce the time IT is required to help support end users, reducing call times by 15 minutes per incident.

As previously noted, the dollar value of the benefit will vary from organization to organization, and many may experience greater benefits. The lowered time and effort to remediate incidents will vary with:

- › The number of employee's end points protected and the average number of incidents seen in the cloud application environment per year.
- › The average time spent to remediate incidents prior to Cloud App Security.
- › How the organization leverages Cloud App Security to help remediate incidents.
- › The fully loaded compensation of SecOps, IT staff, and end users.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a conservative three-year risk-adjusted total PV of \$6.4 million.



**80%**  
Reduction in time to  
discover and remediate  
cloud-based incidents

## Lowered Time And Effort To Remediate Incidents: Calculation Table

| REF. | METRIC  | CALCULATION   | YEAR 1             | YEAR 2             | YEAR 3             |
|------|---|---|--------------------|--------------------|--------------------|
| B1   | Total number of employee's end points protected by MCAS                             | Assumes 10% growth YoY  | 30,000             | 33,000             | 36,300             |
| B2   | Average number of incidents per year  | Assumes growth YoY as threats get smarter (rounded value shown) | 2,000              | 2,538              | 3,300              |
| B3   | Threats automatically eliminated with MCAS due to policies                          | B2*75% (rounded value shown)                                    | 1,500              | 1,904              | 2,475              |
| B4   | Remaining threats requiring remediation   | B2-B3 (rounded value shown)                                     | 500                | 635                | 825                |
| B5   | Baseline person-hours to discover and remediate cloud-based incidents prior to MCAS | Mean-time-to-know + mean-time-to-remediate                      | 96                 | 96                 | 96                 |
| B6   | Reduction in time with MCAS   | Interview finding   | 60%                | 70%                | 80%                |
| B7   | SecOps hourly salary  | A3  | \$65               | \$65               | \$65               |
| B8   | <b>Reduction in SecOps time and effort to remediate incidents</b>                   | <b>B4*B5*B6*B7</b>  | <b>\$1,872,000</b> | <b>\$2,772,000</b> | <b>\$4,118,400</b> |
| B9   | Help desk call time avoided   | B4*.25 hours per incident (rounded value shown)                 | 125                | 159                | 206                |
| B10  | IT help desk hourly salary  |   | \$44               | \$44               | \$44               |
| B11  | Blended end user hourly salary  |   | \$42               | \$42               | \$42               |
| B12  | <b>IT help desk and end user time savings</b>                                       | <b>B9*(B10+B11)</b>   | <b>\$10,750</b>    | <b>\$13,644</b>    | <b>\$17,738</b>    |
| Bt   | Lowered time and effort to remediate incidents                                      | B8+B12  | \$1,882,750        | \$2,785,644        | \$4,136,138        |
|      | Risk adjustment   | ↓10%  |                    |                    |                    |
| Btr  | Lowered time and effort to remediate incidents (risk-adjusted)                      |   | \$1,694,475        | \$2,507,080        | \$3,722,524        |

## Improved Ability To Avoid Data Breach

SecOps must consider phishing, malware, compromised accounts, and the leak of sensitive data when thinking about their cloud application environments. Prior to investing in Cloud App Security, the interviewed organizations lacked the visibility to understand their risk postures. With Cloud App Security, they now have the tools to detect and protect against an actual breach – whether it's detecting and alerting against abnormal user behavior, alerting against potentially compromised accounts with investigation priority, closely monitoring all native and OAuth apps, or detecting and remediating attempted malware attacks in real time. Utilizing Cloud App Security, organizations protect against security threats, better protect their data, and ensure and authorize correct user access.

To consider the impact of a data breach within the composite organization, Forrester assumes:

- › Each employee end point has access to 250 sensitive data assets with an average value of \$10 per data asset.



**40%**  
Reduction in likelihood of a breach to data assets with MCAS

- › The likelihood of a breach without Cloud App Security is about 1.5%. This will vary based on industry, but Forrester chose to make a conservative estimate about the probability of a breach.
- › With Cloud App Security, the composite organization is able to reduce the likelihood of a data breach by 30% in Year 1. As the SecOp team creates more policies and adds more automation to threat detection process, this improves to 40% by Year 3, reducing the likelihood of a data breach to less than 1% with Cloud App Security.
- › To calculate the value of the benefit, Forrester considered the potential cost of a breach without Cloud App Security versus the cost of a breach with Cloud App Security.

While we focus on the value of the data assets protected by Cloud App Security for this calculation, when you're considering the impact within your own organization, it is important to consider both the value of your data assets (which may differ based on the sensitivity and type of data and industry) as well as the potential effects and cost ramifications beyond the value of the data asset. That includes brand perception, lost customers, and other business impacts. This may have a significant impact on the value of this benefit to your organization.

Due to this, the benefit can vary with:

- › The size, industry, region, and other factors of an organization that may impact the value of its data assets or the likelihood of a breach.
- › The severity of a security event.
- › How the organization leverages Cloud App Security to help detect and protect against cyberthreats.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a conservative three-year risk-adjusted total PV of over \$1.6 million.

| Improved Ability To Avoid Data Breach: Calculation Table |  |   |            |            |            |
|--|--|---|------------|------------|------------|
| REF.   | METRIC   | CALCULATION                                   | YEAR 1     | YEAR 2     | YEAR 3     |
| C1   | Number of data assets protected                          | 250 sensitive data assets per employee device | 3,750,000  | 4,125,000  | 4,537,500  |
| C2   | Average value of data asset                              |   | \$10       | \$10       | \$10       |
| C3   | Potential impact of breach                               | C1*C2   | 37,500,000 | 41,250,000 | 45,375,000 |
| C4   | Likelihood of breach without MCAS                        |   | 1.5%       | 1.5%       | 1.5%       |
| C5   | Potential cost of breach without MCAS                    | C3*C4   | \$562,500  | \$618,750  | \$680,625  |
| C6   | Reduction in likelihood of breach with implementing MCAS |   | 30%        | 35%        | 40%        |
| C7   | Potential cost of breach with MCAS                       | C5*C6   | \$168,750  | \$216,563  | \$272,250  |
| Ct   | Improved ability to avoid data breach                    | C5-C7   | \$393,750  | \$402,188  | \$408,375  |
|  | Risk adjustment  | ↓15%  |            |            |            |
| Ctr  | Improved ability to avoid data breach (risk-adjusted)    |   | \$334,688  | \$341,859  | \$347,119  |

## Improved Compliance And Audit Reporting

Prior to investing in Cloud App Security, ensuring compliance and audit reporting was a painful, time-consuming, and manual task for the



interviewed organizations, and that affected workers across SecOps, IT, and auditing. With Cloud App Security, the teams can easily assess the risk and compliance of their existing applications and ensure they meet any internal or external security and compliance requirements. Cloud App Security provides the composite organization access to a centralized dashboard for governance and policy enforcement, enabling it to capture a detailed audit trail — such as who has accessed what information and data, which greatly reduces the time required to audit activities.



For the composite organization, Forrester assumes:

- › Each year, there are four audits (one per quarter) that involve SecOps, IT, and internal auditing.
- › Based on findings from the interviews, it would take about 160 person-hours to compile details related to cloud applications for audits prior to Cloud App Security. With Cloud App Security, the hours required to prepare for these audits is reduced by 90%.
- › Forrester assumes a blended fully loaded annual salary of \$150,000 for the SecOps and IT staff and auditors involved.

**90%**  
Reduction in time spent  
on audits with MCAS

The dollar value of this benefit will vary from organization to organization, and many may experience greater benefits. The savings from improved compliance and audit reporting will vary with:

- › The number of audits per year.
- › The number of person-hours it takes to prepare for an audit event.
- › The salary of those individuals involved.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a conservative three-year risk-adjusted total PV of \$98,135.

#### Improved Compliance And Audit Reporting: Calculation Table

| REF. | METRIC  | CALCULATION                 | YEAR 1    | YEAR 2    | YEAR 3    |
|------|---|-----------------------------|-----------|-----------|-----------|
| D1   | Number of audits per year                                     | Assumption                  | 4         | 4         | 4         |
| D2   | Person-hours spent on compiling auditing details without MCAS | Interviews                  | 160       | 160       | 160       |
| D3   | Reduction in time spent on audits with MCAS                   | Interviews                  | 90%       | 90%       | 90%       |
| D4   | Blended salary of SecOps and IT staff and internal auditors   |                             | \$150,000 | \$150,000 | \$150,000 |
| Dt   | Improved compliance and audit reporting                       | $D1 * D2 * D3 * D4 / 2,080$ | \$41,538  | \$41,538  | \$41,538  |
|      | Risk adjustment   | ↓5%                         |           |           |           |
| Dtr  | Improved compliance and audit reporting (risk-adjusted)       |                             | \$39,462  | \$39,462  | \$39,462  |

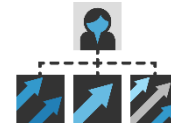
### Optimized Resources

With features like automatic configuration, policy-setting, improved visibility, and easier management, Cloud App Security helps organizations reduce the time it takes to manage cloud application security operations. Due to this, existing staff members are able to monitor, assess, and govern their cloud application environment easily and without the need for additional headcount. Even as threats continue to get smarter and increase each year, Cloud App Security ensures that the organization will not require more FTEs to manage its cloud application environment and can use these savings to hire for other openings. With Cloud App Security, the organization avoids investment

in expensive future SecOps hires by improving its cloud security posture management.

For the composite organization, Forrester assumes that:

- › The SecOps team will begin to use Cloud App Security in Year 1.
- › Without Cloud App Security, it is estimated that the composite organization would require at least 0.5 new SecOp FTE hires to manage the changing cloud application portfolio and evolving security threats each year.
- › With Cloud App Security, the composite organization avoids the need for additional headcount for this purpose starting in Year 2 and can use the savings to hire elsewhere in the organization.



This benefit will vary from organization to organization. Depending on the organization's size and Cloud App Security usage, the value of this benefit may be significantly higher. The cost avoidance associated with this benefit will vary with:

- › The size of the deployment, which may require more support.
- › The fully loaded salary of SecOps FTEs.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a conservative three-year risk-adjusted total PV of \$111,291.

**0.5 FTEs**  
 Avoided SecOp hires each year due to improved ability to manage cloud

**Optimized Resources: Calculation Table**

| REF. | METRIC   | CALCULATION                        | YEAR 1 | YEAR 2    | YEAR 3    |
|------|--|------------------------------------|--------|-----------|-----------|
| E1   | Reallocated SecOp hires due to improved ability to manage cloud app security |                                    |        | 0.5       | 0.5       |
| E2   | SecOps annual salary   | \$100,000 * 1.35 benefits modifier |        | \$135,000 | \$135,000 |
| Et   | Optimized resources  | E1*E2                              |        | \$67,500  | \$67,500  |
|      | Risk adjustment  | ↓5%                                |        |           |           |
| Etr  | Optimized resources (risk-adjusted)  |                                    |        | \$64,125  | \$64,125  |

**Flexibility**

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement Microsoft Cloud App Security and later realize additional uses and business opportunities, including:

- › **Using cloud security posture management capabilities to protect the IaaS environment.** While not directly discussed as part of the study, a major future benefit for organizations would be for those organizations that use Cloud App Security to assess their security configurations across their IaaS environments. Doing so will increase the benefits by ensuring organizations can properly monitor and protect their IaaS environments.
- › **Increasing number of protected devices.** Organizations can further improve the business value they receive by adding additional end points to see wider cloud application security.

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

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a future additional investment. This provides an organization with the "right" or the ability to engage in future initiatives but not the obligation to do so.

# 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 |
| Ftr         | Licensing costs                       | \$0     | \$1,260,000 | \$1,386,000 | \$1,524,600 | \$4,170,600 | \$3,436,364   |
| Gtr         | Implementation and ongoing management | \$957   | \$39,811    | \$39,811    | \$39,811    | \$120,391   | \$99,962      |
|             | Total costs (risk-adjusted)           | \$957   | \$1,299,811 | \$1,425,811 | \$1,564,411 | \$4,290,991 | \$3,536,326   |

## Licensing Costs

For the composite organization, Forrester uses the list price of \$3.50 per user per month. The composite organization protects all its employee's end points each year. It purchases 30,000 licenses in Year 1, growing to 36,300 licenses in Year 3. That yields a three-year total PV of more than \$3.4 million.

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total costs to be a PV of more than \$3.5 million.

While Cloud App Security is available to purchase as a standalone product at the licensing costs shown below, it is important to note that many organizations have access to Cloud App Security as part of their Microsoft 365 E5 licensing without incurring additional expense. It is also available in other bundles across EMS E3, EMS E5, and Microsoft 365 E5 Security.

### Licensing Costs: Calculation Table

| REF. | METRIC                                   | CALCULATION       | YEAR 1      | YEAR 2      | YEAR 3      |
|------|--|-------------------|-------------|-------------|-------------|
| F1   | Annual licensing costs for MCAS per user | \$3.50/user/month | \$42        | \$42        | \$42        |
| F2   | Number of users                          | B1                | 30,000      | 33,000      | 36,300      |
| Ft   | Licensing costs                          | F1*F2             | \$1,260,000 | \$1,386,000 | \$1,524,600 |
|      | Risk adjustment                          | 0%                |             |             |             |
| Ftr  | Licensing costs (risk-adjusted)          |                   | \$1,260,000 | \$1,386,000 | \$1,524,600 |

## Implementation And Ongoing Management

The interviewed organizations reported relatively low implementation and support efforts associated with Cloud App Security, but this varies based on the size of the organization. For the composite organization:

- › Initial implementation requires 15 person-hours. For many organizations running Microsoft 365 E5, this was included in the overall implementation. Ongoing management of the solution itself requires an average of 12 person-hours per week.

These costs can vary with:

- › The size of the deployment, which may require more implementation and support hours.
- › The average hourly salary of IT.

To account for these risks, Forrester adjusted this cost upward by 10%,

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

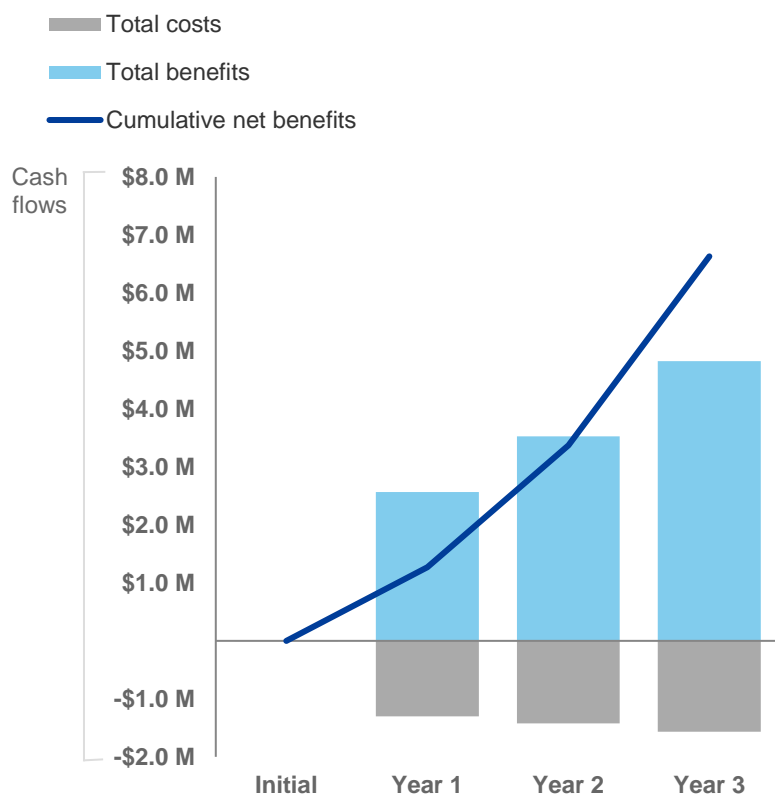
yielding a three-year risk-adjusted total PV of \$99,962.

| <b>Implementation And Ongoing Management: Calculation Table</b> |   |   |         |          |          |          |
|---|---|---|---------|----------|----------|----------|
| REF.  | METRIC  | CALCULATION   | INITIAL | YEAR 1   | YEAR 2   | YEAR 3   |
| G1  | Implementation  | Person-hours  | 15      |          |          |          |
| G2  | Ongoing management                                    | 12 hours per week   |         | 624      | 624      | 624      |
| G3  | IT hourly salary                                      | (\$90,000 * 1.35X benefits modifier)/2,080 working hours per year (rounded) | \$58    | \$58     | \$58     | \$58     |
| Gt  | Implementation and ongoing management                 | $G1+G2*G3$  | \$870   | \$36,192 | \$36,192 | \$36,192 |
|   | Risk adjustment                                       | ↑10%  |         |          |          |          |
| Gtr   | Implementation and ongoing management (risk-adjusted) | (Rounded)   | \$957   | \$39,811 | \$39,811 | \$39,811 |

# 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             | (\$957) | (\$1,299,811) | (\$1,425,811) | (\$1,564,411) | (\$4,290,991) | (\$3,536,326) |
| Total benefits          | \$0     | \$2,567,580   | \$3,528,619   | \$4,824,548   | \$10,920,746  | \$8,885,248   |
| Net benefits            | (\$957) | \$1,267,768   | \$2,102,808   | \$3,260,137   | \$6,629,756   | \$5,348,922   |
| ROI                     |         |               |               |               |               | 151%          |
| Payback period (months) |         |               |               |               |               | <3            |





# Microsoft Cloud App Security: Overview

The following information is provided by Microsoft. Forrester has not validated any claims and does not endorse Microsoft or its offerings.

Microsoft Cloud App Security is Microsoft's CASB, fully and uniquely integrated with Microsoft Threat, Identity and Information Protection solutions while providing world-class productivity to end users. The integrations in first-party applications are extended by the breadth of integrations to third-party applications, infrastructure, and platforms.

Microsoft Cloud App Security manages and controls session risk for SaaS applications, provides visibility and data protection across IaaS and PaaS resources, and creates control-plane management for all your cloud resources. With quick and easy access to compliance data for every application that gets accessed from your environment, you'll have cutting-edge tools at your fingertips, ready for you to deploy policies and encourage appropriate use of your environment's technology and the risk assessments you need to make crucial decisions about how to best manage your environment.

## Microsoft Cloud App Security

|   |  |  |  |
|---|--|--|--|
| <br><b>Identity &amp; access management</b><br>Secure identities to reach zero trust | <br><b>Threat protection</b><br>Help stop damaging attacks with integrated and automated security | <br><b>Information protection</b><br>Locate and classify information anywhere it lives | <br><b>Security management</b><br>Strengthen your security posture with insights and guidance |
|---|--|--|--|

### How to get started:

- › Sign up for a [free trial](#) of Microsoft Cloud App Security.
- › Upload a log file from your network firewall or enable logging via [Microsoft Defender ATP](#) to [discover shadow IT](#) in your network and assess the risks of detected cloud apps.
- › [Connect your Cloud Apps](#) to Microsoft Cloud App Security to detect suspicious user activity and exposed sensitive data.
- › Enable out-of-the-box [anomaly detection policies](#) and start detecting cloud threats in your environment.
- › Continue with more advanced use cases across [Information Protection](#), Compliance and more.

### Resources:

- › Visit our Website: [aka.ms/mcas](https://aka.ms/mcas)
- › Join the conversation on Tech Community: [aka.ms/mcascommunity](https://aka.ms/mcascommunity)
- › Stay up to date and subscribe to our blog: [aka.ms/mcasblog](https://aka.ms/mcasblog)
- › Learn more about Microsoft Cloud App Security: [aka.ms/mcastech](https://aka.ms/mcastech)
- › Get started with a free trial: [aka.ms/mcastrial](https://aka.ms/mcastrial)
- › Understand your licensing options: [aka.ms/mcaslicensing](https://aka.ms/mcaslicensing)

# 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.