A Forrester Total Economic Impact™
Study Commissioned By Microsoft
September 2018

The Total Economic Impact™ Of Microsoft Office 365 Threat Intelligence

Cost Savings And Business Benefits Enabled By Threat Intelligence As Part Of Office 365 E5

FORRESTER®

Table Of Contents

Project Director:
Adrienne Capaldo

ABOUT FORRESTER CONSULTING

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

FORRESTER®

Key Benefits

IT hours saved due to improved detection and response of security threats:
27,168 hours each year

Reduced likelihood of a security breach:
60%

Reduction in time required for investigation and remediation with Office 365 Threat Intelligence:
89.3%

Executive Summary

Organizations must create a sophisticated system to protect against the ever-increasing threat of cyberattacks. Microsoft Office 365 Threat Intelligence enhances threat protection by enabling organizations to better detect, analyze, remediate, and educate against cyberthreats and improving its customers' overall security. Organizations found significant benefits from leveraging Threat Intelligence as part of their Microsoft Office 365 E5 deployment. 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 Office 365 Threat Intelligence. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Office 365 Threat Intelligence on their organizations. To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed three customers and surveyed an additional 50 users of Office 365 Threat Intelligence.

Prior to deploying Office 365 E5 with Threat Intelligence, the interviewed and surveyed customers typically used many disparate third-party solutions to handle email and data file protection, resulting in complex security environments that were both expensive and difficult to manage. One key insight uncovered during interviews and through surveys was that organizations improve their overall security and get the most value of their investment when using Threat Intelligence as part of the Office 365 E5 license. This integrated suite of security products provides a holistic approach to security, providing end-to-end cyber protection. Threat Intelligence integrates seamlessly with other Office 365 features like Exchange Online Protection and Advanced Threat Protection to bring greater security to an organization. With the move to Office 365 E5, organizations leveraged Threat Intelligence to create a more secure, easier-to-manage security environment that not only decreased costs but provided actionable insights and improved the overall security of these organizations. Office 365 Threat Intelligence leverages the "Microsoft Intelligent Security Graph," which utilizes AI capabilities to analyze and continuously learn from billions of data points across Microsoft's ecosystem to better understand and provide actionable insights against potential security threats.

Forrester developed a composite organization based on data gathered from the customer interviews and surveys to reflect the total economic impact that Office 365 Threat Intelligence has on an organization. The composite organization is representative of these organizations and is used to present the aggregate financial analysis for this study.

Key Findings

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

FORRESTER®

ROI
186%

Benefits PV
$4.2 million

NPV
$2.7 million

Payback
6 months

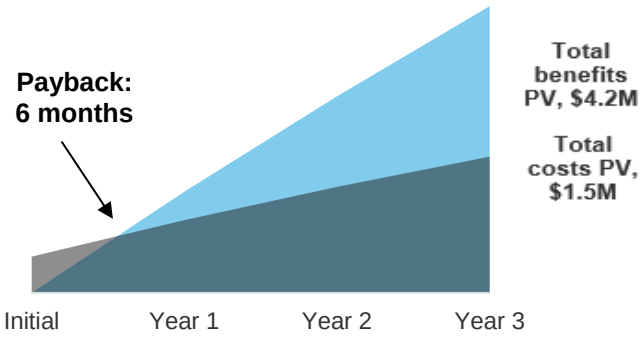
- **Avoided IT costs of over $673K due to consolidation of security systems.** With the deployment of Office 365 E5, organizations can consolidate their security solutions onto a single platform, reducing licensing costs expended on a myriad of third-party security solutions. With Threat Intelligence, these organizations gain full visibility into their email, collaboration applications, and Windows Defender ATP ecosystems, resulting in significant time savings for the security operations teams, as they no longer need to manage and maintain multiple third-party security solution software or vendors. Beyond the cost reduction, this consolidation of security systems enables organizations to create “a single pane of glass” into their security environments, resulting in three-year risk adjusted avoided costs of $673,848.
- Reduced the severity and impact of end user security events, saving 27,168 hours of IT support time each year. By implementing Office 365 E5, organizations can leverage Threat Intelligence to greatly reduce the time-to-action and number of hours spent on remediation of phishing and malware events, resulting in a significant decrease in the impact and number of successful attacks. With Threat Intelligence, the time necessary for remediation events is reduced by 50 hours; with faster time-to-action, organizations also eliminate 528 security events annually. Organizations reduce both the severity and number of successful end user security events, yielding a three-year risk-adjusted total PV of over $1.9 million.
- **Reduced end user downtime, resulting in savings of nearly $1.27M.** With the reduction in both the number and severity of security events also comes a reduction in end user downtime. With Office 365 Threat Intelligence, users are less likely to be impacted by malware of phishing attacks that require downtime, such as manual remediation or complete refresh for their device, eliminating 6 hours of downtime per user each year.
- **Reduced the likelihood of a data breach, resulting in savings of over $321K in value.** Malware and phishing attacks create a considerable risk of a serious data breach that could have wide-reaching business impacts on an organization. With Office 365 Threat Intelligence, organziations reduce the likelihood of a data breach by 60%.

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

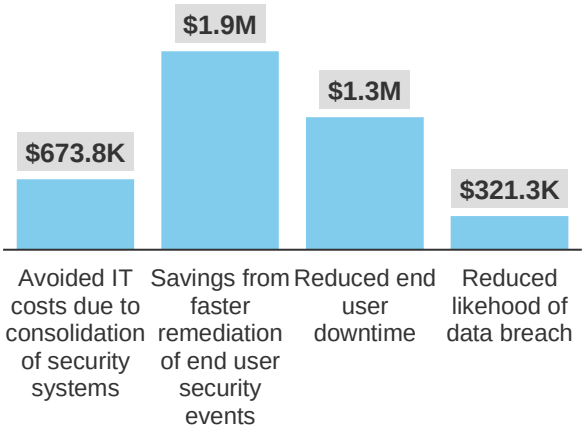
- **Licensing for 6,000 total mailboxes.** These represent costs paid to Microsoft for the use of Office 365 Threat Intelligence, at a rate of $8 per mailbox per month, resulting in a total risk-adjusted cost over the three years analyzed of $1.43 million.
- **Implementation, ongoing support, and training costs totaling $22K over three years.** These represent the mix of internal and external costs associated with Office 365 Threat Intelligence’s implementation, ongoing support, and training.

Forrester’s interviews with three existing customers, survey of 50 customers, and subsequent financial analysis found that an organization based on these customers experienced benefits of $4.2 million over three years versus costs of $1.5 million, adding up to a net present value (NPV) of $2.7 million and an ROI of 186%.

Financial Summary



Benefits (Three-Year)



FORRESTER®

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 and survey, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing Microsoft Office 365 Threat Intelligence.

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 Office 365 Threat Intelligence can have on an organization:

DUE DILIGENCE
Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to Office 365 Threat Intelligence.

CUSTOMER INTERVIEWS AND SURVEY
Interviewed three organizations and surveyed 50 organizations using Office 365 Threat Intelligence to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION
Designed a composite organization based on characteristics of the interviewed and surveyed organizations.

FINANCIAL MODEL FRAMEWORK
Constructed a financial model representative of the interviews and survey using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewed organizations.

CASE STUDY
Employed four fundamental elements of TEI in modeling Microsoft Office 365 Threat Intelligence'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 Office 365 Threat Intelligence.

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 Office 365 Threat Intelligence Customer Journey

BEFORE AND AFTER THE OFFICE 365 THREAT INTELLIGENCE INVESTMENT

Interviewed Organizations

For this study, Forrester conducted three interviews with Microsoft Office 365 Threat Intelligence customers. In addition, Forrester surveyed 50 customers to better understand the challenges, results, key benefits, and costs associated with the Office 365 Threat Intelligence investment. Many of the interviewed and survey respondents were using Office 365 Threat Intelligence as part of their overall Office 365 E5 licensing. All respondents met the following selection criteria:

- They were headquartered in North America or the UK.
- Each respondent was an IT decision maker responsible for cybersecurity within their organization.
- They had 500 or more employees; the majority of respondents had 2,000 or more employees.
- Annual revenue ranged from less than $100M to more than $5B.
- They represent a wide variety of industries, including manufacturing, professional services, healthcare, and telecommunications.

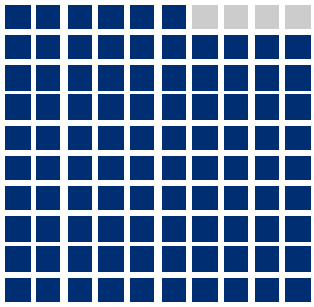
> "Phishing is a major problem for us, like everybody else, and the ability to be able to identify mailboxes that receive the particular phishing attack and pull the message from those mailboxes before some number of them click on it, was a big factor in our investment."
>
> *Enterprise architect, financial services*

Key Drivers

The interviewed and surveyed organizations highlighted several key drivers that led them to invest in Office 365 E5 and Threat Intelligence:

› The organizations wanted to be able to better identify, monitor, and understand cyberthreats and minimize the risk associated with them. Protecting users from a wide variety of security threats is becoming more complicated, and the implications of a data breach are escalating, with both internal and external business impact. Each of the organizations Forrester spoke with noted that the main driver for their investment in Office 365 E5 and Threat Intelligence was to improve their overall security and minimize the risk associated with cyberthreats. As these organizations began to study their existing security landscapes and road map their desires for the future, they understood that they needed to do more to protect their organizations. An enterprise architect at a financial services organization discussed the organization's current and future security landscape: "It was decided that having a simple signature-based product was not sufficient to protect us from the persistent threats. So, then we started an investigation into, 'Okay, can we invest in more sophisticated security products to do enterprise detection and response?'" The enterprise architect added, "Phishing is a major problem for us, like everybody else, and the ability to be able to identify mailboxes that receive the particular phishing attack and pull the message from those mailboxes before some number of them click on it, was a big factor in our investment." In fact, due to the wide-ranging implications of a security incident or data breach, enterprise security professionals are

Threat Intelligence helps us better understand the risks and threat landscape of our organization.



96%
Of security professionals agree

FORRESTER®

tasked with the difficult job of ensuring that not only internal employees are protected, but that their ability to protect their internal team ensures the trust and security of their end customers. The financial services organization summed it up: "People have to trust us to take care of them, and it requires us to have a certain level of overall security. The better we are at doing cybersecurity and keeping track of those threats and avoiding them and remediating them quickly, the more trustworthy we will be at least to the regulators, and in the end, the general public." The ability to identify, monitor, understand, and minimize the risk associated with cyberattacks was a key goal in the investment in Office 365 E5 and Threat Intelligence.

- **Third-party solutions created a complex environment that was a burden on existing IT resources.** Many of the organizations hoped to reduce the operational complexity that had existed within their security landscapes and were looking to consolidate their solutions to create more integrated and more cost-effective security environments. Organizations found that it was often a heavy burden on their security operations teams to manage and maintain the many disparate systems that made up their security solutions. This also created an issue in which there was not central visibility across all the solutions, often leading to a fragmented view of the threat landscape. This lack of visibility was a point of frustration for IT professionals as it took a significant amount of time and effort to investigate, monitor, and remediate threats.

> "I think much of the value for us as a company is in the fact that it's a more coherent and more integrated landscape than we could ever achieved with all kinds of third-party solutions."
>
> *Enterprise architect, financial services*

- **The companies were interested in leveraging new technologies but were operating within tight IT budget constraints.** While these organizations were up against budgetary and resource constraints, there was also a lot of interest in exploring how leveraging new technologies such as artificial intelligence and machine learning could impact and improve their cybersecurity. Many of the IT security professionals Forrester spoke with were interested in understanding how they could invest in a solution across the continuously evolving products available to them that would enable them to take advantage of the future benefits of AI, but in a cost-effective environment. Organizations hoped that through leveraging these types of technologies, they could have more insights and automation around understanding and remediating their threat landscapes in the future.

> "We're a small team, and I think the goal of getting machine learning and AI to better recognize these attacks and automate a response . . . I think that would certainly help us with the small staff size. We can take advantage of those machine learning/AI capabilities in order to maximize what our team is able to do."
>
> *IT security director, education*

Key Results

After an evaluation period, the interviewed organizations selected Office 365 Threat Intelligence. The interviews and survey data revealed that key results from the Office 365 Threat Intelligence investment include:

- **Improved overall security.** Across interviews and surveys, Forrester heard that the leveraging Threat Intelligence as part of their investment in Office 365 E5 led to an improvement in the organizations' overall security. The IT security director in the education industry told us, "With the use of Threat Intelligence, we experience fewer losses, have less incident response costs internally and in terms of outside council, forensics groups, because Threat Intelligence has effectively reduced risk and reduced successful attacks and mitigated damages." Threat Intelligence captures data from the Microsoft Intelligent Security Graph to ensure greater visibility across the threat landscape and help organizations better detect threats. Threat Intelligence creates actionable insights for these organizations that helped them to

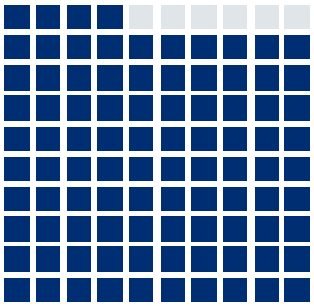
investigate, monitor, and ultimately protect against cyberthreats. For example, describing an incident the organization had encountered earlier that day, one organization told us: "This morning, the incident was probably 90% remediated within 15 minutes of us being alerted to it. That's not something we could do at all before Threat Intelligence." With real-time and customizable threat alert notifications, organizations are better able to respond to incidents. Across the board, organizations greatly reduced the number of hours spent on investigation and remediation with the investment in Threat Intelligence and reported this helped them to reduce the number of successful malware and phishing attacks. Forrester heard from one organization: "Remediation is definitely faster. And not even is it just faster, but we have far more capabilities now for remediation. In a lot of cases in the past, there was nothing we could now. Now, with Threat Intelligence, it's quick and extremely capable."

While the focus of this study is specifically on the value of Office 365 Threat Intelligence, one key insight uncovered during interviews and through surveys was that organizations improve their overall security and get the most value of their investment when using Threat Intelligence as part of the Office 365 E5 license. This integrated suite of security products provides a holistic approach to security, providing end-to-end cyberprotection. Threat Intelligence integrates seamlessly with other Office 365 features like Exchange Online Protection and Advanced Threat Protection to bring greater security to an organization. One organization utilizing Threat Intelligence as part of its E5 license told us: "It's the integration between these products that gives them extra value. They gave us capabilities that would not have been able to afford in the past. And the fact that they're integrated with each other and sharing information back and forth to some degree makes this much more valuable".

- **Reduced costs associated with licensing and support.** The investment in Office 365 E5 with Threat Intelligence enabled these organizations to reduce many of the costs and time associated with identifying, monitoring, and remediating threats by consolidating the solutions required for these tasks. Threat Intelligence brought many capabilities together under one cost-effective solution for interviewed organizations: "Threat Intelligence's capabilities are something we didn't have before, and because of the bundle that Microsoft put together, this was affordable for us at the scale that we needed to do it." Organizations saw great value in consolidating on a trusted platform. The financial services organization told us, "We value best of suite over best of breed. We also trust Microsoft. We've seen their track record, we've talked to these guys, we are in touch with this group regularly, we believe that we have the same vision that they will bring us forward. They will become part of a much more holistic approach to our enterprise security."

  Beyond the reduction in licensing costs through eliminating many third-party solutions, Threat Intelligence reduced the time required for management and maintenance of these systems. With Threat Intelligence, organizations can now view prospective threats through a "single pane of glass," creating greater visibility and understanding into prospective threats. Specifically, Office 365 Threat Intelligence has helped organizations gain deeper visibility into their email, collaboration applications, and Windows Defender ATP ecosystems. Features like the threat dashboard enable organizations to quickly and

We can better protect our users with Threat Intelligence's security recommendations based on user behaviors.



94%
Of security professionals agree

"If we were to buy individual products that had all the same capabilities, we would have to spend so much more. In reality, we would not be able to afford it. I believe this was a very good use of the funds that we did have available to us. It gave us far more capability than we could've gotten with that level of funding from competitors."

Information security engineer, education

easily understand in a visual format what threats have been addressed. Survey results revealed that 86% of IT security professionals agreed that the threat dashboard enabled them to quickly and accurately understand potential threats. By consolidating onto Threat Intelligence, the security team can more easily monitor and investigate threats, reducing the burden on the staff. In addition, with more proactive monitoring capabilities and recommendation for remediation, organizations can act more quickly and cost-effectively on remediation efforts.

Not only did Threat Intelligence reduce costs for the IT organization, but it also improved the end user's experience by minimizing downtime. One organization, regarding the reduction in downtime, stated: "I fully believe that we have prevented compromised accounts using these tools. I would think dozens, maybe hundreds, of accounts over the last six months have not been comprised because of this toolset, and for those individuals, there is definite savings, as we would have to shut their account down previously."

- **Leveraged new AI technology to improve overall understanding and remediation of cyberthreats.** With new artificial intelligence and machine learning features, Office 365 E5 enables organization to leverage Microsoft's continuously learning and improving algorithms to protect against threats. One organization described to us that "one of Microsoft's big selling points for us, they have so many million data points that the longer this is out there, the smarter it is going to get; if we talk a year from now, it may be that we're getting significantly larger benefits than we are receiving today." Threat Intelligence leverages Microsoft Intelligent Security Graph, which analyzes billions of data points across the Office 365 ecosystem to better understand malware and phishing campaigns, to educate organizations on key factors like top targeted users, malware frequency, and security recommendations. As Threat Intelligence continues to grow its use of these features, organizations will be able to more easily understand and automate response to threats, reducing the number of attacks, costs associated with support, and the likelihood and severity of data breaches.

"Our strategy is twofold: First it is to prevent any current attacks and to understand what is happening and who the culprits are. Second, it is to be proactive and strive to put up a barrier against any future unknown types of threats or attacks."

Survey respondent, professional services

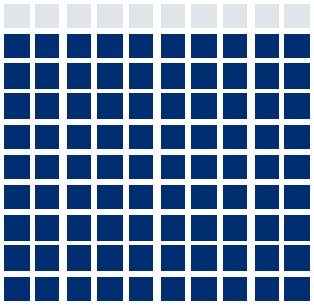
Composite Organization

Based on the interviews and survey, 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 three companies that Forrester interviewed and the 50 organizations Forrester surveyed, and it is used to present the aggregate financial analysis in the next section. The composite organization that Forrester synthesized from the customer data has the following characteristics:

Description of composite. The composite organization is a global organization with most of its operations in North America and Europe. The organization has 7,000 total employees. Out of those, 5,000 employees utilize Office 365 E5 solutions. There are 6,000 mailboxes, including individual and shared accounts, that utilize Office 365 solutions.

Deployment characteristics. The composite organization moved its 6,000 mailboxes from disparate third-party solutions to Office 365 E5. Specifically, the organization leveraged the following components of Threat Intelligence: Threat Tracker; Threat Dashboard; Threat Explorer, and Threat Intelligence Reports.

Threat Intelligence's use of machine learning algorithms helped us mitigate phishing campaigns.



90%
Of security professionals agree

Key assumptions
5,000 employees
6,000 mailboxes

FORRESTER®

Analysis Of Benefits

QUANTIFIED BENEFIT DATA AS APPLIED TO THE COMPOSITE

Total Benefits

REF.	Benefit	Initial	Year 1	Year 2	Year 3	Total	Present Value
Atr	Avoided IT costs due to consolidation of security systems	$0	$223,594	$272,813	$326,250	$822,656	$673,848
Btr	Savings from faster remediation of end user security events	$0	$764,100	$764,100	$764,100	$2,292,300	$1,900,204
Ctr	Reduced end user downtime	$0	$510,000	$510,000	$510,000	$1,530,000	$1,268,295
Dtr	Reduced likelihood of data breach — business impact	$0	$118,150	$129,965	$141,780	$389,896	$321,341
	Total benefits (risk-adjusted)	**$0**	**$1,615,844**	**$1,676,878**	**$1,742,130**	**$5,034,852**	**$4,163,687**

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 $4.1 million.

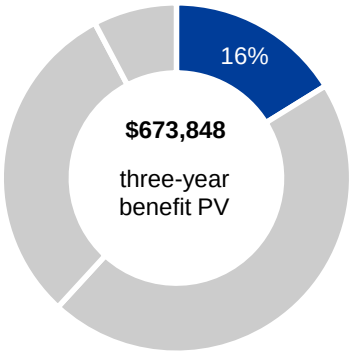
Avoided IT Costs Due To Consolidation Of Security Systems

With a full suite of end user security features and functionality, Office 365 E5 enables organizations to protect against cyberthreats from one single solution instead of multiple third-party solutions. With the deployment of Office 365 E5, Threat Intelligence supports organizations as they consolidate their security solutions onto a single platform, reducing licensing costs expended on a myriad of third-party security solutions. Interviewees and survey respondents reported a range of eliminated licensing costs from $25,000 to $600,000.

This consolidation into a single solution also results in significant time savings for the security operations teams, as they no longer need to manage and maintain multiple third-party security solution software or vendors. Beyond the cost reduction, this consolidation of security systems enables organizations to create “a single pane of glass” into their security environment. With Threat Intelligence, organizations gain full visibility into their email, collaboration applications, and Windows Defender ATP ecosystems. Further, the security operations team no longer needs to review many different systems to gain a full understanding of the threat landscape and gain greater efficiency and effectiveness in the investigation, monitoring, and remediation of issues.

Forrester assumes that:

- Initially, the composite organization eliminates licensing costs of $200,000 on third-party security solutions. As the organization becomes more proficient at leveraging Office 365 E5 with Threat Intelligence, it continues to decrease its reliance on other security solutions, increasing to $300,000 in decreased licensing costs by Year 3.
- Likewise, there is a reduction in the time spent by the security professionals responsible for managing and maintaining those solutions. Initially, that time is reduced by 775 hours annually, increasing to 1,000 hours by Year 3 as the organization continues to eliminate those third-party solutions.
- An average hourly fully loaded salary of $62.50 is used for IT FTEs.



Avoided IT costs:
16% of total benefits

FORRESTER®

The avoided costs due to consolidation of security systems can vary with:

- The licensing costs associated with third-party security solutions.
- The number of hours required to support and maintain those solutions.
- The fully loaded hourly salary of IT security professionals.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $673,848.

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.

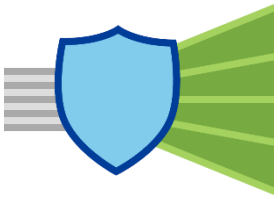
Avoided IT Costs Due To Consolidation Of Security Systems: Calculation Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	Avoided third-party security solution costs		$200,000	$250,000	$300,000
A2	Avoided hours of IT effort to support and maintain third-party security solutions		775	850	1,000
A3	Average hourly IT salary		$62.50	$62.50	$62.50
At	Avoided IT costs due to consolidation of security systems	A1+(A2*A3)	$248,438	$303,125	$362,500
	Risk adjustment	↓10%			
Atr	**Avoided IT costs due to consolidation of security systems (risk-adjusted)**		**$223,594**	**$272,813**	**$326,250**

Savings From Faster Remediation Of End User Security Events

By implementing Office 365 E5 with Threat Intelligence, organizations reduce both the severity and impact of end user security events. Some organizations reported nearly a 100% reduction in the number of security events they experienced with Office 365 E5 compared to their previous environments. With the implementation of Office 365 E5, organizations across the board could leverage Threat Intelligence to greatly reduce the time-to-action and number of hours spent on remediation of phishing and malware events, resulting in a significant decrease in the impact and number of successful attacks. Organizations leveraged the Threat Intelligence dashboard to provide better visibility into and investigate prospective attacks; with its use of the Microsoft Intelligent Security Graph, Threat Intelligence enables organizations to detect potential threats and make recommendations based on user behavior patterns, enabling security teams to proactively monitor and defend against many attacks. In fact, 90% of survey respondents agreed that Office 365's use of machine learning algorithms mitigated phishing campaigns. With real-time customizable threat alert notifications, the security operations teams could act quickly. Additionally, Threat Intelligence enables organizations to better understand threats, act, and remediate attacks to decrease the severity of the attack, reducing the number of successful malware and phishing attacks.

To calculate the value of this benefit, Forrester assumes that:



89.3% reduction in the investigation and remediation with Threat Intelligence

- Before Office 365 Threat Intelligence, the composite organization spent 56 hours per end user security event on investigation and remediation. With Threat Intelligence, the composite organization reduces the time spent on investigation remediation to 6 hours per event, resulting in a time savings of 50 hours per security event.
- Based on survey and interview results, the composite organization experienced 1,008 end user security events annually (84 per month) prior to its investment in Office 365. With Office 365, this number decreases to 480 annually, resulting in the elimination of 528 security events annually.
- An average hourly fully loaded salary of $62.50 is used for IT FTEs.
- As not all time saved translates into additional, value-add work, only 50% of this benefit is realized.

To understand the total benefit associated with the savings from faster remediation of end user security incidents, Forrester calculates out the time saved from completely avoided security incidents, as well as the time saved on remediation for remaining security events.

The reduction in security events will be affected by:

- The number and severity of malware or phishing attacks.
- The average hourly salary of IT.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of over $1.9 million.

Savings From Faster Remediation Of End User Security Events: Calculation Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
B1	Hours per event to investigate and remediate before Threat Intelligence		56	56	56
B2	Hours per event to investigate and remediate after Threat Intelligence		6	6	6
B3	**Total hours saved on remediation due to Threat Intelligence**	**B1-B2**	**50**	**50**	**50**
B4	Number of end user security events before Office 365 E5	84 per month	1,008	1,008	1,008
B5	Number of end user security events with Office 365 E5	40 per month	480	480	480
B6	**Total number of eliminated events**	**B4-B5**	**528**	**528**	**528**
B7	Hours saved from eliminated events	B2*B6	3,168	3,168	3,168
B8	Hours saved on remaining events	B3*B5	24,000	24,000	24,000
B9	**Total number of hours saved**	**B7+B8**	**27,168**	**27,168**	**27,168**
B10	Average IT hourly salary		$62.50	$62.50	$62.50
B11	Productivity capture		50%	50%	50%
Bt	Savings from faster remediation of end user security events	B9*B10*B11	$849,000	$849,000	$849,000
	Risk adjustment	↓10%			
Btr	**Savings from faster remediation of end user security events (risk-adjusted)**		**$764,100**	**$764,100**	**$764,100**

Reduced End User Downtime

With the reduction in both the number and severity of security events also comes a reduction in end user downtime. Previously, when impacted by a malware or phishing attack, end users more frequently required either manual remediation or a complete refresh for the device. Time estimates ranged from 2 hours to greater than a day for these instances. With Office 365 Threat Intelligence, users are less likely to be impacted by malware of phishing attacks that require downtime. The detection and remediation features within Threat Intelligence ensure that downtime is kept to a minimum for the employees, while helping the IT team better understand how to quickly address the issue.

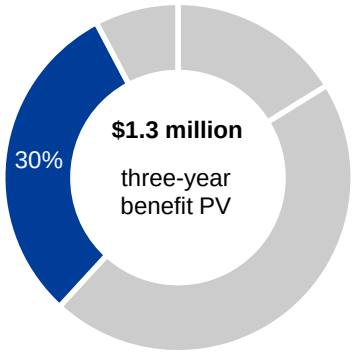
For the composite organization, Forrester assumes that:

- Each of the 5,000 Threat Intelligence users experiences an average of 1.5 downtime events per year, based on survey and interview feedback.
- Each downtime event causes an average of 4 hours of downtime. With the implementation of Office 365 Threat Intelligence, users avoid this downtime.
- An average hourly fully loaded salary of $40 represents a blended rate across workers.
- Again, as not all time saved translates into additional, value-add work, only 50% of this benefit is realized.

The reduction in end user downtime can vary with:

- The number of Office 365 Threat Intelligence users.
- The rate and severity of malware of phishing attacks.
- The mean-time-to-remediation.
- The fully burdened salary of end users.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of nearly $1.3 million.



Reduced end user downtime:
30% of total benefits

Reduced End User Downtime: Calculation Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
C1	Total number of users		5,000	5,000	5,000
C2	Average number of downtime events per year		1.5	1.5	1.5
C3	Average end user downtime per event	Hours	4	4	4
C4	Average end user fully loaded hourly salary		$40	$40	$40
C5	Percent productivity capture		50%	50%	50%
Ct	Reduced end user downtime	C1*C2*C3*C4*C5	$600,000	$600,000	$600,000
	Risk adjustment	↓15%			
Ctr	**Reduced end user downtime (risk-adjusted)**		**$510,000**	**$510,000**	**$510,000**

FORRESTER®

Reduced Likelihood Of A Data Breach — Business Impact

Malware and phishing attacks create a considerable risk of a serious data breach that could have wide-reaching business impacts on an organization. For this benefit, Forrester focuses specifically on the business impact costs associated with a successful security breach. In the Ponemon Insitute's "2017 Cost of Data Breach Study," the average lost customer business from a breach is $1.69 million — however, in the US, it is signficantly higher at $4.13 million.[1] The average cost to communicate with the affected third parties is $205,000. Together, the cost is nearly $1.9 million per incident in business impact. Through the use of Office 365 Threat Intelligence, organizations protect themselves against a major data breach by better understanding the threat landscape, improved monitoring of potential threats, and decreased effort required to remediate an issue to quickly suppress the risk for a larger data breach.

For the composite organization, Forrester assumes that:

- The average business impact of a data breach is over $1.89 million.
- Based on research conducted by the Ponemon Institute, the probability of a data breach is 13.85%.
- Based on feedback from the interviews and surveys, the likelihood of a data breach is reduced by 60% by Year 3 as organizations improve their use of Threat Intelligence and can better proactively monitor their threat landscapes.

This benefit can vary with:

- The size, industry, region, and other factors of an organization that may impact the business impact costs associated with a data breach.
- The severity of malware of phishing attacks.
- An organization's ability to leverage Threat Intelligence to detect threats.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of nearly $321,341.

60% reduction in the likelihood of a data breach with Threat Intelligence

Reduced Likelihood Of A Data Breach — Business Impact: Calculation Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
D1	Average business impact of data breach		$1,895,714	$1,895,714	$1,895,714
D2	Average probability of a data breach occurrence		13.85%	13.85%	13.85%
D3	Reduced likelihood of a data breach with Office 365 Threat Intelligence		50.0%	55.0%	60.0%
Dt	Reduced likelihood of data breach — business impacts	D1*D2*D3	$131,278	$144,406	$157,534
	Risk adjustment	↓10%			
Dtr	**Reduced likelihood of data breach (risk-adjusted)**		**$118,150**	**$129,965**	**$141,780**

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 Office 365 Threat Intelligence and later realize additional uses and business opportunities, including:

- **Education and training offerings.** Organizations understand that a key component of threat protection is training end users to recognize and correctly react and respond to potential threats. With new features like attack simulator, the organization can test, in a controlled environment, different types of realistic attacks on end users to better understand where the company may require more training. Furthermore, this tool can educate end users and prevent the potential for a future security breach.
- **Utilizing the newest offerings from Microsoft Office 365 Threat Intelligence.** Microsoft is continually innovating on new product features and functionality. For example, Threat Intelligence will be increasing its use of automation features, like automated incidence response to address security incidents. Functionality such as this will help users maximize the business impact of their Office 365 E5 investments.
- **Increasing user base.** Organizations can further improve the business value they receive by adding additional users to see wider security efficiency and effectiveness throughout the organizations.

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
Etr	Licensing costs	$0	$576,000	$576,000	$576,000	$1,728,000	$1,432,427
Ftr	Implementation, ongoing support, and training costs	$5,775	$6,825	$6,825	$6,825	$26,250	$22,748
	Total costs (risk-adjusted)	**$5,775**	**$582,825**	**$582,825**	**$582,825**	**$1,754,250**	**$1,455,175**

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 $1.45 million.

Licensing Costs

For the composite organization, Forrester uses the list price of $8 per license per month. The composite organization purchases a total of 6,000 licenses to protect its individual and shared mailboxes.

While Office 365 Threat Intelligence is available as an add-on at the licensing costs shown below, it is important to note that many organizations have access to Threat Intelligence through their Office 365 E5 licensing.

Licensing Costs: Calculation Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
E1	Number of licenses		6,000	6,000	6,000
E2	Annual cost	$8 per month	$96	$96	$96
Et	Licensing costs	E1*E2	$576,000	$576,000	$576,000
	Risk adjustment	0%			
Etr	**Licensing costs (risk-adjusted)**		**$576,000**	**$576,000**	**$576,000**

Implementation, Ongoing Support, and Training Costs

Organizations reported relatively low implementation and support effort required, but this ranged based on the size of the organization. Likewise, the training required depended on the size of the security operations team and other individuals who needed to be trained on the solution. For the composite organization:

- Initial implementation requires 24 person-hours; for many organizations running E5, this was part of the overall Office 365 implementation. Ongoing support requires 96 person-hours per month.
- Additionally, the eight members of the security operations team join 8 hours of training on how to use the solution. To account for 10% turnover, the model accounts for an additional training session for new members of the security operations staff each year.

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.

These costs can vary with:

- The size of the deployment, which may require more implementation and support hours.
- The number of team members requiring training.
- The average hourly salary of IT.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of $22,748.

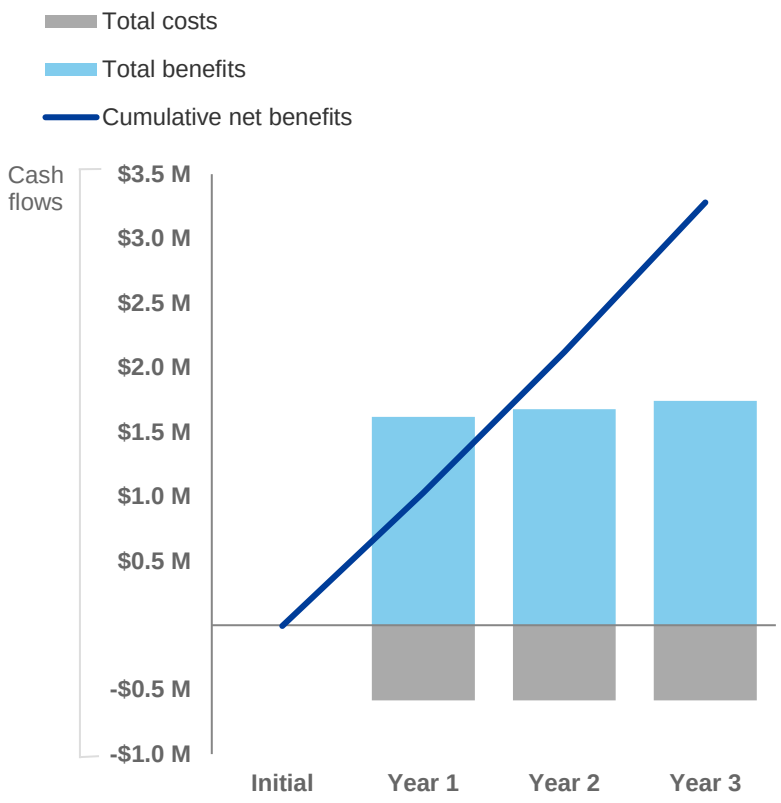
Implementation, Ongoing Support, And Training Costs: Calculation Table

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
F1	Implementation	Person-hours	24			
F2	Ongoing support	Person-hours		96	96	96
F3	Number of trainees		8	1	1	1
F4	Time spent training	Hours	8	8	8	8
F5	Average fully loaded IT salary		$62.50	$62.50	$62.50	$62.50
Ft	Implementation, ongoing support and training costs	F1+F2+(F3*F4)*F5	$5,500	$6,500	$6,500	$6,500
	Risk adjustment	↑5%				
Ftr	**Implementation, ongoing support and training costs (risk-adjusted)**		**$5,775**	**$6,825**	**$6,825**	**$6,825**

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 Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($5,775)	($582,825)	($582,825)	($582,825)	($1,754,250)	($1,455,175)
Total benefits	$0	$1,615,844	$1,676,878	$1,742,130	$5,034,852	$4,163,687
Net benefits	($5,775)	$1,033,019	$1,094,053	$1,159,305	$3,280,602	$2,708,513
ROI						186%
Payback period						6 months

FORRESTER®

Microsoft Office 365 Threat Intelligence: Overview

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

Office 365 Threat Intelligence helps security operations and administrators protect their organizations' Office 365 users by:

- Making it easy to identify, monitor, and understand attacks.
- Helping to quickly address threats in Exchange Online and SharePoint Online.
- Providing insights and knowledge to prevent attacks against their organizations.

Office 365 Threat Intelligence is a collection of insights and information available in the Office 365 Security & Compliance Center. These insights can help your organization's security team protect Office 365 users from attacks. Office 365 Threat Intelligence monitors signals and gathers data from multiple sources, such as user activity, authentication, email, compromised PCs, and security incidents. Business decision makers and Office 365 global administrators, security administrators, and security analysts can all use the information Office 365 Threat Intelligence provides to understand and respond to threats against Office 365 users and intellectual property.

The Threat Dashboard (also referred to as the Security Dashboard) allows users to quickly see what threats have been addressed, and as a visual way to report to business decision makers how Office 365 services are securing your business.

Use the Threat Explorer to analyze threats, see the volume of attacks over time, and analyze data by threat families, attacker infrastructure, and more. The Threat Explorer is the starting place for any security analyst's investigation workflow.

Use the Incidents list to see a list of in-flight security incidents. Incidents are used to track threats such as suspicious email messages and to conduct further investigation and remediation.

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] Source: “2017 Cost of Data Breach Study,” Ponemon Institute, June 2017.