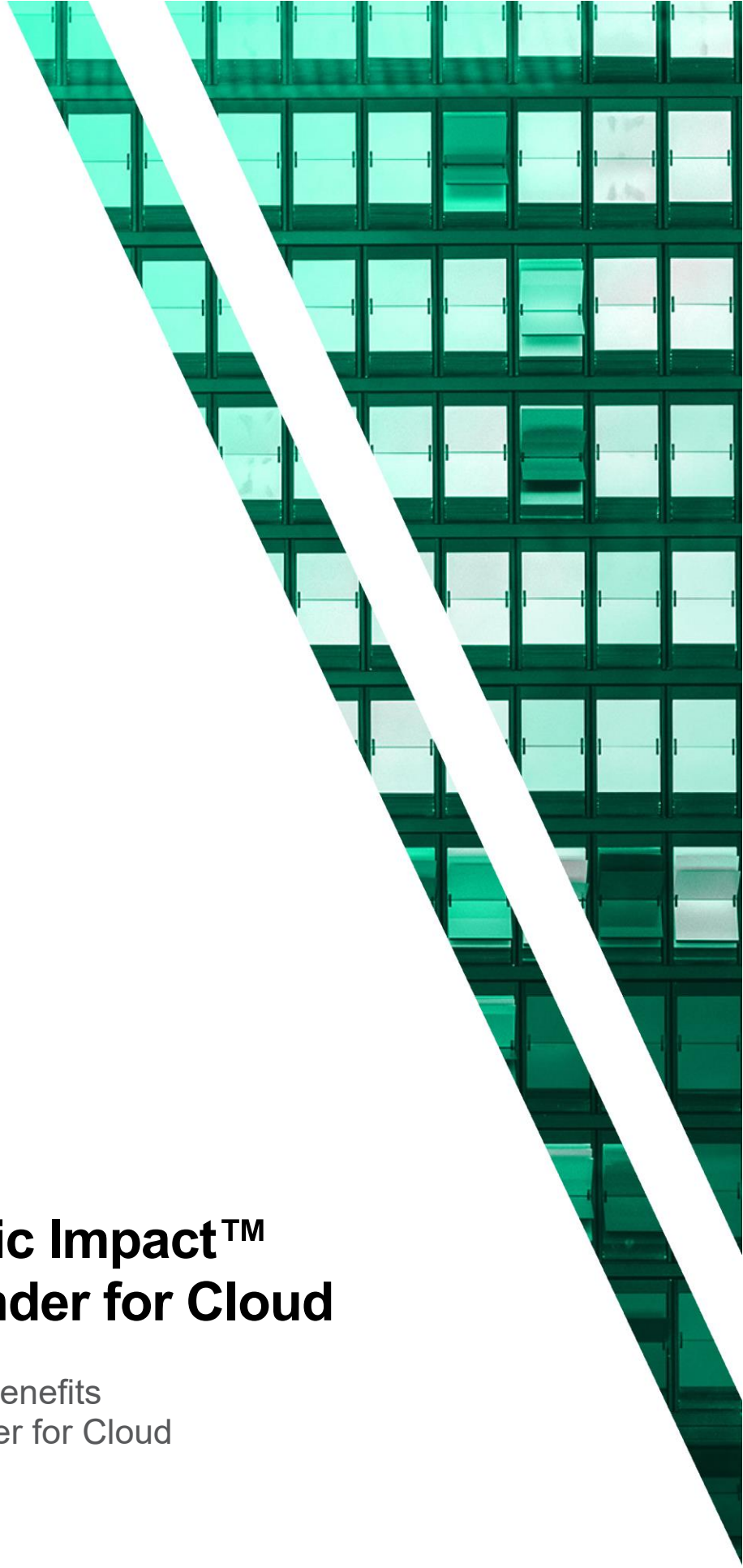
FORRESTER®



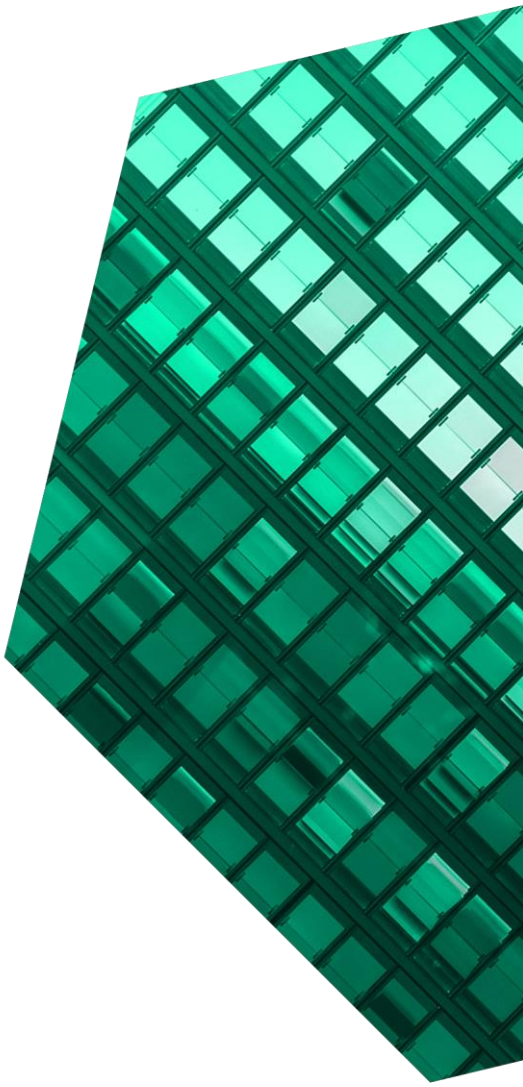
The Total Economic Impact™ Of Microsoft Defender for Cloud

Cost Savings And Business Benefits Enabled By Microsoft Defender for Cloud

FEBRUARY 2021

Table Of Contents

Consulting Team: Nick Mayberry



ABOUT FORRESTER CONSULTING

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

Executive Summary

Microsoft Defender for Cloud provides cloud security posture management and cloud workload protection for Azure and hybrid cloud workloads. With Microsoft Defender for Cloud, organizations reduced their risk of a security breach to cloud workloads by up to 25%, decreased their time to cloud threat mitigation by 50%, sped up security policy and compliance-related workloads by up to 30%, and reduced their spending on third-party security tools and services by over $200,000 annually.

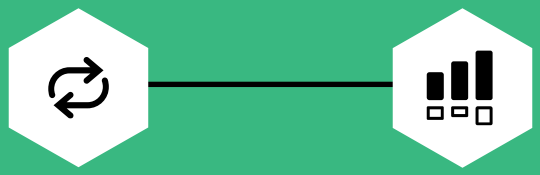
Microsoft Defender for Cloud provides cloud security posture management and cloud workload protection in an integrated tool. Cloud security posture management provides a quantified representation of a customer organization's cloud security posture, with actionable insights for security posture improvement, and enhanced visibility into network asset inventory, while cloud workload protection offers threat detection and response as it relates to cloud-based assets.

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 Microsoft Defender for Cloud. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Microsoft Defender for Cloud on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four customers with experience using Microsoft Defender for Cloud. For the purposes of this study, Forrester aggregated the experiences of the interviewed customers and combined the results into a single composite organization.

Prior to using Microsoft Defender for Cloud, the interviewed customers were relying on multiple third-party cloud security tools that were implemented in different organizational siloes to understand their security posture and defend against potential threats.

KEY STATISTICS



Return on investment (ROI)
219%

Net present value (NPV)
$2.44M

However, the distributed and disintegrated nature of this approach introduced: 1) inefficiencies into security workflows; 2) a plethora of false-positive threat alerts; and 3) limited visibility of the organization's overall security posture.

After the investment in Microsoft Defender for Cloud, the customers' visibility into the security posture of their Azure workloads increased substantially, thereby reducing the risk of cloud security breaches and improving the productivity of security teams responsible for threat detection and remediation and regulatory compliance.

Total benefits PV

$3.6 million

KEY FINDINGS

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

- **Reduced risk of a cloud security breach by up to 25%.** By improving visibility into an organization's security posture across all of its Azure workloads and decreasing time to threat remediation, interviewed organizations shared that they were able to reduce the risk of cloud security breaches. Organizations which are similar in size to those that Forrester interviewed typically experience 1.9 breaches annually at a cost of over $5 million to remediate post-breach. Organizations also experience approximately 3.9 hours of lost productivity per breach among affected employees.[1]
- **Reduced time to threat mitigation by 50%.** Organizations that chose to Microsoft Defender for Cloud's threat detection and response capabilities shared that they were able to decrease their mean time to threat remediation by 50%. They were also able to reduce the number of threats needing remediation by 86%, thanks to false-positive threat alert reduction.
- **Reduction in time spent on security policy and compliance management up to 30%.** Microsoft Defender for Cloud also reduced the amount of time spent on updating security policies and compliance-related workflows by between 20% and 30%. This resulted in the improved productivity of security administrators.
- **Reduced cost of third-party security tools and services from consolidation by over $200,000 annually.** Customers shared that they reduced their spending and reliance on third-party security tools and services. Customers saved 20% to 30% on third-party security tools, reduced third-party security services by $180,000, and reduced third-party penetration test services by 50%.

> **"Without Microsoft Defender for Cloud, we would be in a totally different scenario. We would not have the same insight into what security posture changes we should make."**
>
> — Cloud security specialist, retail

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

- **Reduced risk of noncompliance.** Customers improved their compliance posture with the added visibility and accessibility of regulatory compliance status through Microsoft Defender for Cloud. They also were able to make recommended fixes to improve compliance they might have otherwise missed.
- **Avoided cost of deployment and maintenance.** By choosing a security solution that is native to the Azure cloud, and offloading the related deployment and maintenance work to Microsoft, customers avoided costs they would otherwise had incurred from on-premises solutions and potentially with third-party cloud solutions.
- **Improved threat intelligence and automation.** Customers not only benefitted from shifting workloads like technology implementation, deployment, and maintenance onto Microsoft, but they also benefitted from the fact that Microsoft's scale and telemetry data enable it to update security recommendations and to generate alerts of important threats at speed.

Costs. Risk-adjusted PV costs include:

- **Cost of Microsoft Defender for Cloud.** Microsoft Defender for Cloud's security posture, compliance, and asset inventory assessments are free to Azure subscribers. Threat detection and remediation capabilities come at an additional cost, which is based on the workloads protected.
- **Cost of training and ongoing management.** Customers described requiring 2 hours for adequate training of their security team members in Microsoft Defender for Cloud. One FTE was required to spend 2 hours weekly to manage the solution on an ongoing basis.

The customer interviews and financial analysis found that a composite organization experiences benefits of $3.56M over three years versus costs of $1.11M, adding up to a net present value (NPV) of $2.44M and an ROI of 219%.

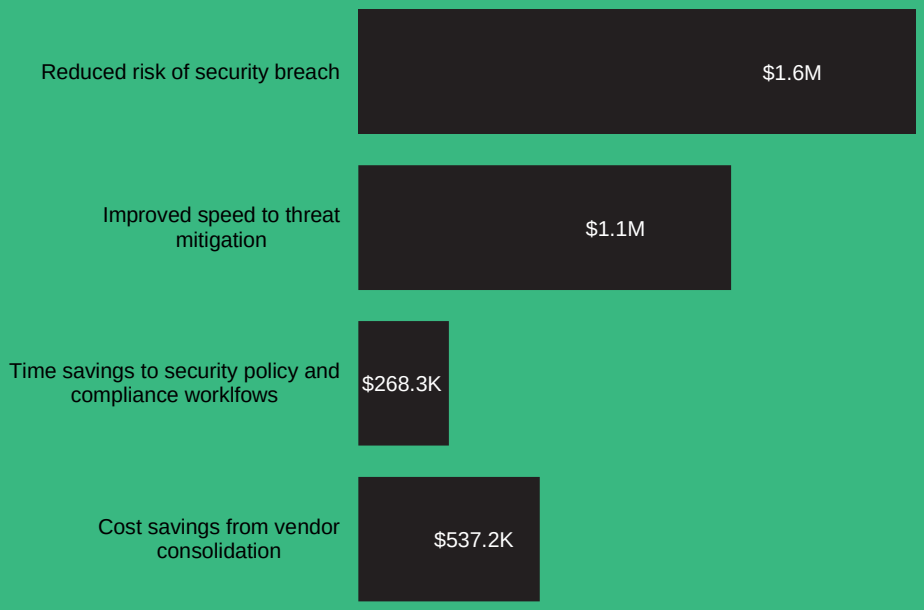
ROI
219%

BENEFITS PV
$3.56M

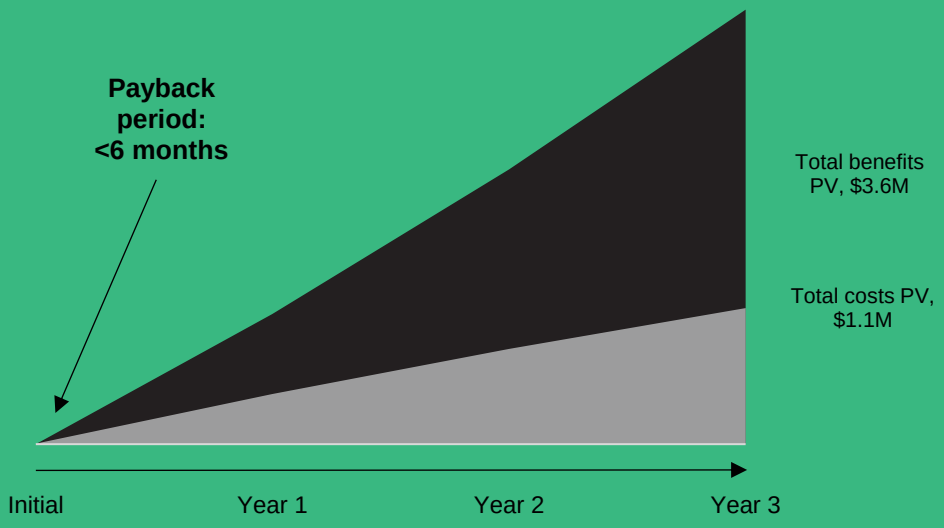
NPV
$2.44M

PAYBACK
<6 months

Benefits (Three-Year)



Financial Summary



TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Microsoft Defender for Cloud.

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 Defender for Cloud can have on an organization.

DUE DILIGENCE

Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to Microsoft Defender for Cloud.

CUSTOMER INTERVIEWS

Interviewed four decision-makers at organizations using Microsoft Defender for Cloud 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 the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Microsoft Defender for Cloud Customer Journey

Drivers leading to the Microsoft Defender for Cloud investment

Interviewed Organizations

Industry	Region	Interviewees	FTEs and **subscription tier**
Enterprise IT	US	Chief information security and privacy officer	500; standard tier
Professional services	EMEA	• Director of technology and security • IT security manager	80,000; free tier
Retail	EMEA	Cloud security specialist	125,000; standard tier
Aerospace	US	Cloud architect	145,000; standard tier

KEY CHALLENGES

Before deploying Microsoft Defender for Cloud, the interviewed organizations described using a variety of third-party security solutions, depending on their stage of transition to the Azure cloud. For customers that deployed Microsoft Defender for Cloud immediately upon shifting workloads to Azure, the prior state consisted of classic on-premises vulnerability tools. For those that had workloads in the Azure cloud prior to deploying Microsoft Defender for Cloud, prior solutions ranged from third-party cloud vulnerability assessment tools to managed service providers hired to monitor and manage cloud vulnerabilities.

The interviewed organizations struggled with common challenges, including:

- **No common source of truth regarding cloud vulnerabilities.** Before deploying Microsoft Defender for Cloud, customers described their security environment being plagued by independent organizational "fiefdoms," with each using multiple, separate third-party security tools. The lack of integration inherent in this segregated environment made a single, trusted common view of organizationwide Azure vulnerabilities nearly impossible. Without this visibility, customers feared the possibility of unknown vulnerabilities putting their organization at risk of a security breach.

> **"Whenever we got a vulnerability report, we'd have a hard time hunting down who was responsible to make sure they would remediate the issue. With Microsoft Defender for Cloud, our teams have full visibility into vulnerabilities and the recommendations that are applicable to them."**
>
> *Cloud security specialist, retail*

- **Security analysts distracted by false-positive threat alerts.** Whether using third-party security tools or having security managed by a service provider, the interviewed customers felt their security teams were spending too much time dealing with false-positive threat alerts. Those with third-party security tools felt that a lack of close integration with the Azure platform prevented these tools from more clearly distinguishing between benign activities and actual threats. And those with managed service providers felt that a lack of understanding from their security teams, in regard to the specifics of

their business, meant that too many non-threatening activities were being sent in for remediation.

"We thought that if we could replace third-party tools with an integrated Azure functionality, it might improve visibility. It might catch additional threats. It might ease configuration work, reducing management overhead in the end."

IT security manager, professional services

SOLUTION REQUIREMENTS

The interviewed organizations searched for a solution that could:

- Provide a unified view regarding security status and vulnerabilities across all Azure and hybrid workloads through a single pane of glass.
- Reduce the number of false-positive threat alerts through closer integration with the Azure platform.
- Save time and resources by introducing automation into security workflows and improving information delivery with a simple and easy-to-use interface.

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and a 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 has the following characteristics:

Description of composite. The composite organization provides business-to-business services to clients of a variety of sizes around the globe. It employs 115,000 people, 20 of whom are security administrators and 10 of whom are security analysts. At the time of deploying Microsoft Defender for Cloud, workloads in Azure represent 25% of total business workloads. The business is remediating approximately 100 potential threats weekly, at a meantime of 6 hours to remediate.

Deployment characteristics. The composite organization began transitioning a number of its workloads to the Azure cloud beginning several years ago. It had previously leveraged a professional services provider to manage and monitor both on-premises security vulnerabilities and those of its increasing Azure workloads. Workloads in Azure are increasing at a rate of about 5% of total workloads annually. As cloud usage increases, the composite organization opts to simplify its cloud security processes and environment by deploying a tool native to the Azure platform: the Microsoft Defender for Cloud.

Key assumptions

- **115,000 FTEs**
- **20 security administrators**
- **10 security analysts**
- **Azure workloads represent 25% of total workloads in Year 1**
- **100 potential threats weekly**
- **6 hours meantime to remediate**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Reduced risk of a security breach	$428,690	$664,221	$946,069	$2,038,980	$1,649,457
Btr	Improved speed to mitigate threats	$443,945	$443,945	$443,945	$1,331,834	$1,104,025
Ctr	Time savings to security policy and compliance workflows	$82,620	$109,620	$136,620	$328,860	$268,349
Dtr	Cost savings from vendor consolidation	$216,000	$216,000	$216,000	$648,000	$537,160
	Total benefits (risk-adjusted)	$1,171,255	$1,433,786	$1,742,634	$4,347,675	$3,558,991

REDUCED RISK OF A SECURITY BREACH

Evidence and data. Customers shared that the Microsoft Defender for Cloud improved their overall security posture and reduced the risk of potential security breaches or otherwise successful security threats. These organizations attributed the following to the Microsoft Defender for Cloud:

- Improved visibility across their Azure and hybrid environments.
- Faster remediation of security threats.
- Improved policy and compliance administration.

"Having one dashboard, one single pane of glass, is easier for teams to consume security information than having several products. We now judge any new tooling by its ability to integrate with Microsoft Defender for Cloud."

Cloud security specialist, retail

In terms of visibility, Microsoft Defender for Cloud provides one dashboard and a single pane of glass for every team to see an organization's security posture, this includes: conformity with and effectiveness of security policies; active, potential, and historical security threats; and the live status of security compliance with regulatory regimes across the organization's entire Azure estate.

Microsoft Defender for Cloud also reduced the meantime to remediation of cloud security threats. In addition to the added visibility of having all Azure-related active, potential, and historical security threats accessible through one dashboard, Microsoft Defender for Cloud limited the number of false-positive threat alerts that distracted security analysts from the more dangerous and likely security threats. Combined, these features reduced the dwell time of security threats and diminished the likelihood of their success.

Finally, Microsoft Defender for Cloud reduced the risk of potential security breaches by improving policy and compliance administration. Microsoft Defender for Cloud provides a trackable, quantifiable metric in Secure Score that represents the solution's

"At the point of discovery of any breach scenario, the breach is less impactful. Over the time it takes you to remediate that threat, the dwell time, the risk increases exponentially. By reducing dwell time, Microsoft Defender for Cloud reduces the risk and the ultimate cost of a breach."

Cloud architect, aerospace

assessment of how well an organization conforms its own resources and subscriptions to its internal security policies and best practices. Additionally, the Microsoft Defender for Cloud will also recommend actions to be taken to improve conformity with these policies and provide automated "quick fixes" to implement these recommendations at the push of a button.

"Our previous security posture reporting was not as quantifiable as Secure Score. It's given me a lot more insights into where we're at and it does so without oversimplification. When I share it with other executives, it's very clear. They can see what our posture is like and where we've got areas of improvement. I've even used it to secure additional budget."

Director of technology and security, professional services

Similarly, the Microsoft Defender for Cloud reports on the organization's compliance with various regulatory regimes, and it improves teams' ability to report on this compliance directly to regulators when necessary.

"We can now demonstrate to regulators our compliance with standards like CIS 10 or ISO on demand. We can also add in custom regulations to report on."

Chief information security and privacy officer, enterprise IT

The combined effect of these improvements is to make a successful security incident less likely.

Modeling and assumptions. Based on the customer interviews, Forrester estimates for the composite organization:

- The average annual number of security breaches is 1.9.[1]
- The average total cost of a security breach is $5,417,220.[1]
- A percentage of total organizational workloads protected by Azure Security Cloud grows from 20% in Year 1, to 25% in Year 2, to 30% in Year 3.
- A risk reduction from Azure Security Cloud grows from 15% in Year 1, to 25% in Year 2, to 30% in Year 3 as security policies are continuously updated and security teams become increasingly effective at utilizing Microsoft Defender for Cloud.
- The prior downtime in hours caused by security breaches are 3.9 hours per breach, or 7.4 hours annually at 1.9 breaches per year (A1).
- Each outage from a security breach effects approximately 15% of the organization.
- The average fully burdened hourly rate of impacted employees is $35.
- The productivity recapture rate is 25%.

Reduction in risk of security breach

25%

Risks. The reduced risk of a security breach will vary with:

- The number and associated costs of security breaches per year.
- The percentage of all the organization's workloads occurring on Azure and protected by Microsoft Defender for Cloud.
- The risk reduction from Microsoft Defender for Cloud given security policy and Microsoft Defender for Cloud usage improvements.
- The average number of downtime hours per outage caused by security breaches.
- The average percentage of the organization impacted by these outages.
- The average fully burdened hourly rate of impacted employees.
- The ability to recapture productivity from these outages.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.6 million.

Reduced Risk Of A Security Breach

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	Average annual number of security breaches	Forrester	1.9	1.9	1.9
A2	Average total cost of a security breach	Forrester	$5,417,220	$5,417,220	$5,417,220
A3	Percent of all workloads protected by Microsoft Defender for Cloud	Interviews	20%	25%	30%
A4	Risk reduction from Microsoft Defender for Cloud	Interviews; Forrester	15%	20%	25%
A5	Subtotal – reduced risk of a security breach	A1*A2*A3*A4	$308,782	$514,636	$771,954
A6	Prior downtime hours per user annually	Forrester; A1*3.9 hours per breach	7.4	7.4	7.4
A7	Number of users affected	15%	17,250	17,250	17,250
A8	Average fully burdened hourly rate per user	Forrester	$35	$35	$35
A9	Productivity recapture rate	Forrester	25%	25%	25%
A10	Subtotal – improved productivity from reduced downtime	A6*A7*A8*A9*A4	$167,541	$223,388	$279,234
At	Reduced risk of a security breach	A5+A10	$476,322	$738,023	$1,051,188
	Risk adjustment	↓10%			
Atr	Reduced risk of a security breach (risk-adjusted)		$428,690	$664,221	$946,069
	Three-year total: $2,038,980			**Three-year present value: $1,649,457**	

IMPROVED SPEED TO MITIGATE THREATS

Evidence and data. As discussed, Microsoft Defender for Cloud improves organizations' response time to potential cloud security threats. Interviewed organizations shared that this improved response times, decreased the risk of a successful security breach, and improved the overall productivity of security analysts and other professionals tasked with remediating threats.

Interviewed organizations shared that time to remediate went from days or weeks to hours or days, depending on the threat. Prior environments were defined by using multiple third-party security tools, which required a number of manual steps to be followed once a security threat was identified, including log search, aggregation, visualization, and dump analysis. Each of these steps needed to be managed by a senior security professional, and the overall process included a lot of unproductive time spent waiting for tasks to be completed and reports to be returned.

> **"Our prior environment would detect a lot of false positives, alerting and escalating incidents or events so that we ended up spending more time putting out false-positive fires than responding to legitimate threats."**
>
> *Chief information security and privacy officer, enterprise IT*

Prior environments were also plagued by an overwhelming number of false-positive threat alerts. One customer described getting approximately 10 alerts a day, 90% of which were false positives that required time to investigate that could have been better spent on the single real threat they were experiencing. Customers described scenarios where false positives led to "alert fatigue" and development processes that attempted to limit false positives failed to achieve much success.

After implementing Microsoft Defender for Cloud, customers described an integrated response environment where Tier 1 analysts could more easily interpret the importance of a threat, tabling less dangerous threats and escalating more dangerous ones. For those threats that required escalation, Tier 1 analysts could immediately share all important information, including logs, net files, the alert itself, and the relevant threat model and inference references. Additionally, customers shared that false-positive alerts were reduced by approximately 86%.

Modeling and assumptions. Based on the customer interviews, Forrester estimates:

- The prior number of mean hours for threat remediation were 6 hours.
- The prior number of threats that required remediation were 100 per week.
- The mean hours to remediation of threats improves to 3 hours after deploying Microsoft Defender for Cloud.
- The number of threats requiring remediation improves to 14 per week.
- The average fully burdened annual salary per security analyst is $135,000, or $68 per hour.
- The productivity recapture rate is 25%.

Reduction in mean time to remediate

50%

Risks. The improved speed to mitigate threats will vary with:

- The current meantime to remediation.
- The current number of threats requiring remediation.
- The average fully burdened rate of security analysts.
- The ability of security analysts to recapture productivity.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $1.1 million.

Improved Speed To Mitigate Threats

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
B1	Prior mean hours to remediation	Interviews	6	6	6
B2	Prior number of threats requiring remediation	Interviews; 100/week	5,200	5,200	5,200
B3	New mean hours to remediation	Interviews	3	3	3
B4	New number of threats requiring remediation	Interviews; 14/week	728	728	728
B5	Security analyst fully burdened hourly rate	$100,000*1.35/ 2,000	$68	$68	$68
B6	Productivity recapture rate	Forrester	25%	25%	25%
Bt	Improved speed to mitigate threats	((B1*B2)-(B3*B4))*B5*B6	$493,272	$493,272	$493,272
	Risk adjustment	↓10%			
Btr	Improved speed to mitigate threats (risk-adjusted)		$443,945	$443,945	$443,945
	Three-year total: $1,331,834			**Three-year present value: $1,104,025**	

TIME SAVINGS TO SECURITY POLICY AND COMPLIANCE WORKFLOWS

Evidence and data. In addition to improving productivity related to threat remediation, Microsoft Defender for Cloud increased productivity for security administration workflows related to security policies and compliance. Customers described automation and consistency as key features driving this productivity increase.

As discussed, Microsoft Defender for Cloud provides a Secure Score that quantifies an organization's conformity to its own security policy and best practices. When making recommendations to improve this Secure Score, Microsoft Defender for Cloud may include the option of implementing a quick fix based on Microsoft's prior experience and informed by its telemetry data. This quick fix automates policy updates and maintenance on behalf of security administrators, allowing them to spend more time on more important security-related workflows.

"With Microsoft Defender for Cloud, we have one tool, out of the box, that is sending recommendations to teams. We just make sure that it's providing the right and correct recommendations, and then we let Microsoft do the rest.."

Cloud security specialist, retail

Microsoft Defender for Cloud also enables customer organizations to develop and implement customized fixes similar to the Microsoft-provided quick fixes, increasing automation and security administrator productivity as they relate to the specifics of the organization's industry or environment. Disparate teams across a single organization can then reliably make security updates that leverage out-of-the-box or customized quick fixes that consistently adhere to security administrator policies.

"Microsoft Defender for Cloud is saving our security administrators between 20% and 30% of their overall work time, each."

Cloud architect, aerospace

Microsoft Defender for Cloud has a similar effect on compliance-related security administration workflows. Customers described prior compliance-related security work involving exporting to CVS files, CVS file formatting and editing for readability, evidence collection, and providing access or guided tours through the Azure environment. After deploying Microsoft Defender for Cloud, customers can easily generate compliance-related reports or simply show their Microsoft Defender for Cloud dashboard with the status of the organization's compliance directly to auditors.

Modeling and assumptions. Based on the customer interviews, Forrester estimates for the composite organization:

- There are 20 security administrators.
- The reduction in policy administration-related labor time from automation grows from 15% in Year 1, to 20% in Year 2, to 25% in Year 3.
- The fully burdened annual rate for security administrators is $120,000, or $60 per hour.
- Three security administrators are tasked with compliance workflows.
- Microsoft Defender for Cloud saves 50% of one week for processes related to SOC 2 compliance.
- Microsoft Defender for Cloud saves 30% of one week for processes related to ISO compliance.
- The productivity recapture rate is 25%.

Reduction in policy and compliance management

20% to 30%

Risks. The time savings to security policy and compliance workflows will vary with:

- The total number of security administrators.
- The fully burdened annual rate of security administrators.
- The number of security administrators tasked with compliance-related workflows.
- The ability of security administrators to recapture productivity.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $268,349.

Time Savings To Security Policy and Compliance Workflows

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
C1	Security administrators (FTEs)	Composite	20	20	20
C2	Reduction in overall labor time from automated policy administration	Interviews	15%	20%	25%
C3	Fully burdened annual rate of security administrator		$120,000	$120,000	$120,000
C4	Improved efficiency of policy administration	C1*C2*C3	$360,000	$480,000	$600,000
C5	Security administrators tasked with compliance	Composite	3	3	3
C6	Reduced labor time for SOC 2 compliance process	1 week saved at 50% time	1%	1%	1%
C7	Reduced labor time for ISO compliance process	1 week saved at 30% time	1%	1%	1%
C8	Improved efficiency of security compliance	(C5*C6*C3)+ (C5*C7*C3)	$7,200	$7,200	$7,200
C9	Productivity recapture rate	Forrester	25%	25%	25%
Ct	Time savings to security policy and compliance workflows	(C4+C8)*C9	$91,800	$121,800	$151,800
	Risk adjustment	↓10%			
Ctr	Time savings to security policy and compliance workflows (risk-adjusted)		$82,620	$109,620	$136,620
	Three-year total: $328,860		**Three-year present value: $268,349**		

COST SAVINGS FROM CONSOLIDATION

Evidence and data. After deploying Microsoft Defender for Cloud, customers decommissioned a variety of third-party cloud security tools, managed service provider services, and vulnerability assessment tools and services. Customers described saving between 25% and 30% of their prior third-party cloud security solution spend, while also diminishing related costs of time, material, and support by between 20% and 30%. One customer whose prior state involved security management by a managed service provider reduced those services at a total value of $110,000 annually. The same customer saved $80,000 annually on a vulnerability assessment tool. Additionally, a customer described reducing their reliance on third-party penetration test services after deploying Microsoft Defender for Cloud, estimating these savings at between $350,00 and $600,000 annually.

Modeling and assumptions. Based on the customer interviews, Forrester estimates:

- A total cost of security-related managed services of $180,000 annually.

- A cost per penetration test of $30,000, with four tests run annually and a reduction in use of these services by half.

Risks. The cost savings from consolidation will vary with:

- The total reduction in usage of managed service providers or third-party security tools.
- The choice to reduce the usage of third-party penetration test services or not.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $537,160.

Cost Savings From Consolidation

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
D1	Reduced cost of professional services related to security	Interviews	$180,000	$180,000	$180,000
D2	Reduced cost of penetration test services	$30,000 per test* 4 tests per year* 50% reduction	$60,000	$60,000	$60,000
Dt	Cost savings from vendor consolidation	D1+D2	$240,000	$240,000	$240,000
	Risk adjustment	↓10%			
Dtr	Cost savings from vendor consolidation (risk-adjusted)		$216,000	$216,000	$216,000
	Three-year total: $648,000			**Three-year present value: $537,160**	

UNQUANTIFIED BENEFITS

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

- **Reduced risk of noncompliance.** Customers described having a better overall compliance posture after deploying Microsoft Defender for Cloud. Thanks to the interface of the Microsoft Defender for Cloud dashboard, and the accessibility into compliance status through a single pane of glass, customers understood their compliance posture and implemented any necessary fixes more readily. Additionally, customers implemented certain compliance fixes related to new technologies that they otherwise might have missed.

> **"Some of the recommendations that Microsoft Defender for Cloud has made around securing our containers and microservices infrastructure we would not have caught as quickly."**
>
> *Chief information security and privacy officer, enterprise IT*

- **Avoided cost of deployment and maintenance.** Because Microsoft Defender for Cloud comes available with the Azure platform and is deployable at the touch of a button, interviewed organizations avoided the added cost of internal implementation and deployment time or any associated professional services fees with Microsoft Defender for Cloud.

> **"With Microsoft Defender for Cloud, we started seeing data flow in the first day after everything was connected versus after months of planning and costs spent on professional services during deployment, with consultants coming back for health checks, etc."**
>
> *Chief information security and privacy officer, enterprise IT*

Customers also avoided the time they would need to manage different security tools, including patching work, service and maintenance, configuring the scanning scope, and onboarding new machines.

> **"There's a lot of activity that goes on with third-party solutions, like deployment, configuration, health management, care, and feeding. We didn't have to do any of that."**
>
> *Chief information security and privacy officer, enterprise IT*

- **Improved threat intelligence and automation.** Customers not only benefitted from shifting workloads like technology implementation, deployment, and maintenance onto Microsoft, but they also benefitted from the fact that Microsoft's scale and telemetry data enable it to update security recommendations and to generate alerts of important threats at speed.

"One of our benefits has been the rapid improvement Microsoft continues to do. There's been such a quick turnaround on configuration and asset changes and updates. We've seen tremendous support from the Microsoft team."

Cloud architect, aerospace

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Microsoft Defender for Cloud and later realize additional uses and business opportunities, including:

- **Multicloud security posture.** Customers described future flexibility benefits from taking advantage of Microsoft's recent extension of Microsoft Defender for Cloud to cover the security posture and threat protection of other cloud platforms. They expect to further reduce both internal and external security costs by consolidating all cloud security operations under the Microsoft Defender for Cloud.

"Now that Microsoft Defender for Cloud covers multicloud offerings, we can centrally manage our other cloud platform security operations all with Microsoft Defender for Cloud."

Chief information security and privacy officer, enterprise IT

- **Simpler integration of security into DevOps.** Interviewed organizations also shared that Microsoft Defender for Cloud helped enable their organization's transition to the more flexible security development operations model. Customers relayed that before deploying Microsoft Defender for Cloud, security functioned as a gate to the development process, with developers needing to consistently rely on and consult with the organizations' security professionals to harden applications. After deployment of Microsoft Defender for Cloud, developers can now take it upon themselves to implement the most recent security policies and harden applications, potentially saving weeks of development time for some customers.

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

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Etr	Cost of Microsoft Defender for Cloud	$0	$440,000	$440,000	$440,000	$1,320,000	$1,094,215
Ftr	Cost of training and ongoing management	$4,136	$6,600	$6,600	$6,600	$23,936	$20,549
	Total costs (risk-adjusted)	$4,136	$446,600	$446,600	$446,600	$1,343,936	$1,114,764

COST OF MICROSOFT DEFENDER FOR CLOUD

Evidence and data. Microsoft Defender for Cloud offers complimentary policy, compliance, and asset management functionality to Azure customers. The ability to do threat detection and management with Microsoft Defender for Cloud comes at a variable added cost depending on the number of servers, SQL instances, transactions, etc., that an organization might need to run Microsoft Defender for Cloud on. Please see Microsoft's Microsoft Defender for Cloud pricing page for exact pricing.

Modeling and assumptions. Forrester estimates for the composite organization:

- The cost of Microsoft Defender for servers is $240,000 annually.
- The cost of Microsoft Defender for storage is $120,000.
- The cost of Microsoft Defender for SQL is $40,000 annually.

Risks. The cost of Microsoft Defender for Cloud will vary with:

- The annual cost of Azure servers, storage, and SQL related to Microsoft Defender for Cloud.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.1 million.

Cost Of Microsoft Defender for Cloud						
Ref.	**Metric**	**Calculation**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Cost of Microsoft Defender for servers			$240,000	$240,000	$240,000
E2	Cost of Microsoft Defender for storage			$120,000	$120,000	$120,000
E3	Cost of Microsoft Defender for SQL			$40,000	$40,000	$40,000
Et	Cost of Microsoft Defender for Cloud	E1+E2+E3	$0	$400,000	$400,000	$400,000
	Risk adjustment	↑10%				
Etr	Cost of Microsoft Defender for Cloud (risk-adjusted)		$0	$440,000	$440,000	$440,000
	Three-year total: $1,320,000			**Three-year present value: $1,094,215**		

COST OF TRAINING AND ONGOING MANAGEMENT

Evidence and data. Customers described experiencing additional time costs from training and ongoing management. These organizations shared that each member of their security teams required on average 2 hours of training in order to be effective with Microsoft Defender for Cloud. After deployment, customers also needed one FTE to spend approximately 2 hours per week managing Microsoft Defender for Cloud.

Modeling and assumptions. Forrester estimates for the composite organization:

- Twenty security administrators and 10 security analysts are needed for a total training team size of 30 FTEs.
- Two hours of training are required.
- One FTE is required for ongoing management.
- Two hours are spent weekly managing Microsoft Defender for Cloud.
- The fully burdened hourly rate is $60 for this FTE.

Risks. The cost of training and ongoing management will vary with:

- The total security team size requiring training.
- The number and time cost of FTEs required for ongoing management.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $20,549.

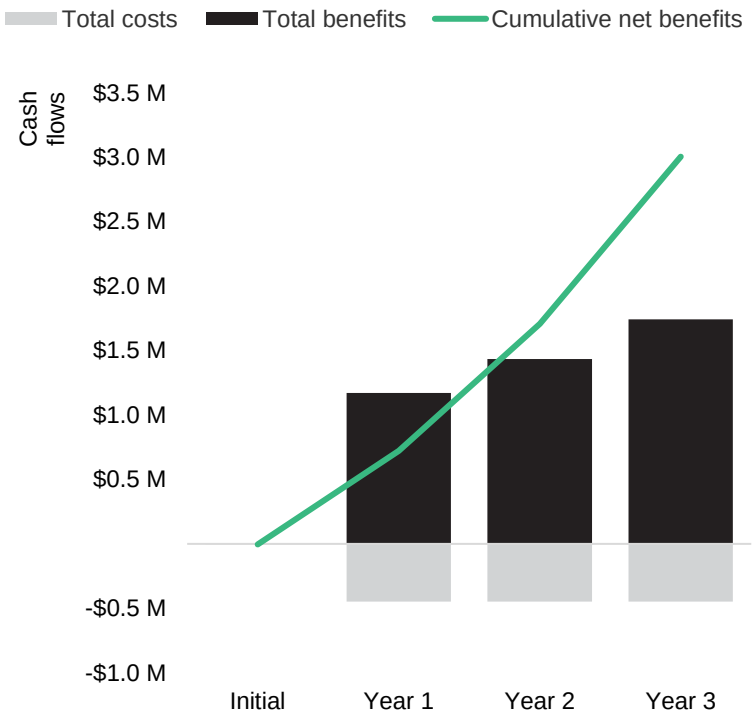
Cost Of Training And Ongoing Management

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
F1	Number of security administrators	C1	20			
F2	Number of security analysts	Composite	10			
F3	Hours required for training	Interviews	2			
F4	Number of FTEs required for ongoing management	Interviews		1	1	1
F5	Weekly hours spent on ongoing management	Interviews		2	2	2
F6	Fully burdened hourly rate per ongoing management FTE	Forrester		$60	$60	$60
Ft	Cost of training and ongoing management	Initial: F1*F3*C3/2,000+ F2*F3*B5 Ongoing: F4*F5*50*F6	$3,760	$6,000	$6,000	$6,000
	Risk adjustment	↑10%				
Ftr	Cost of training and ongoing management (risk-adjusted)		$4,136	$6,600	$6,600	$6,600
	Three-year total: $23,936			**Three-year present value: $20,549**		

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	($4,136)	($446,600)	($446,600)	($446,600)	($1,343,936)	($1,114,764)
Total benefits	$0	$1,171,255	$1,433,786	$1,742,634	$4,347,675	$3,558,991
Net benefits	($4,136)	$724,655	$987,186	$1,296,034	$3,003,739	$2,444,227
ROI						219%
Payback period						<6 months

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

Appendix B: Endnotes

[1] Source: “Cost Of A Security Breach,” Internal Forrester Survey Data, November 2020.


FORRESTER®