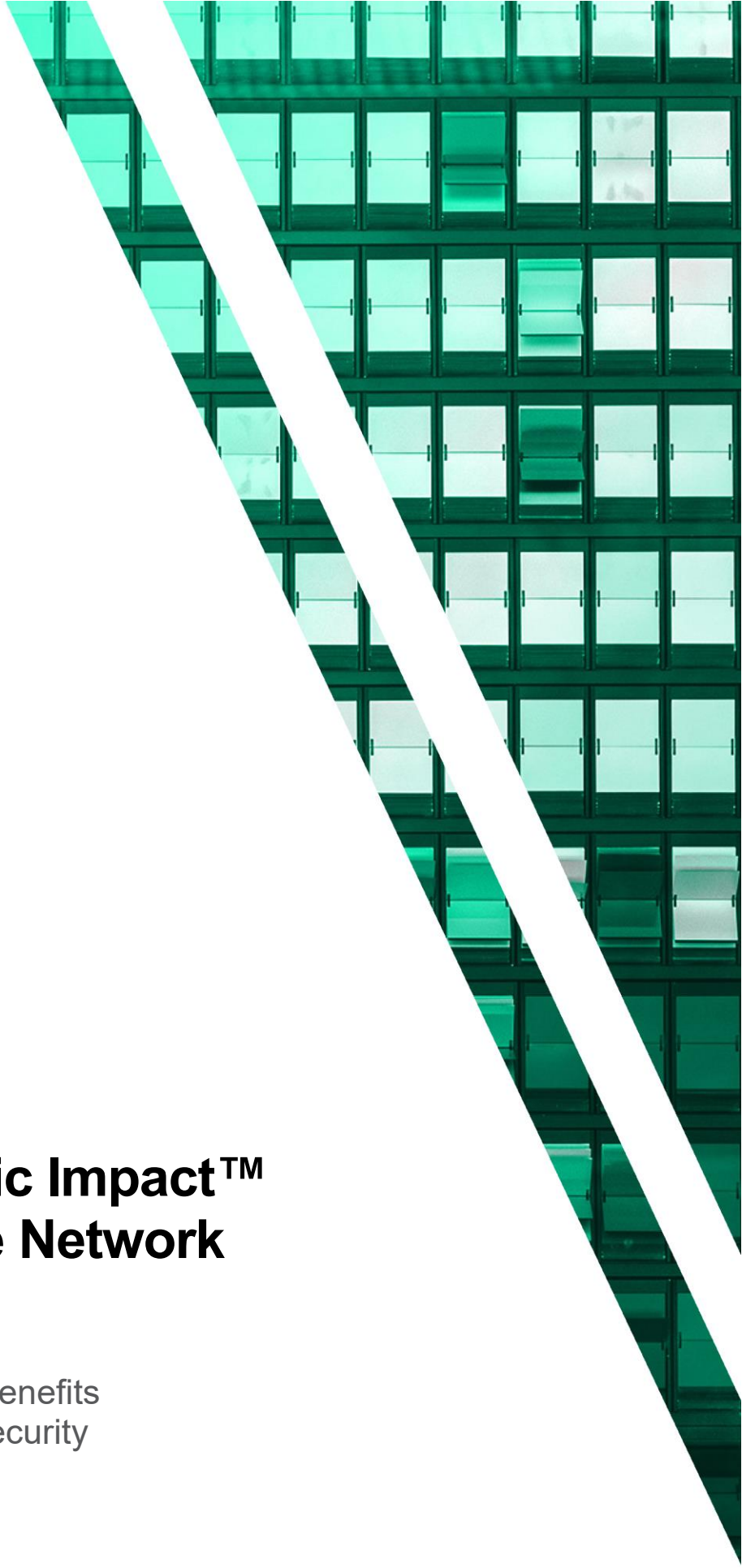
FORRESTER®



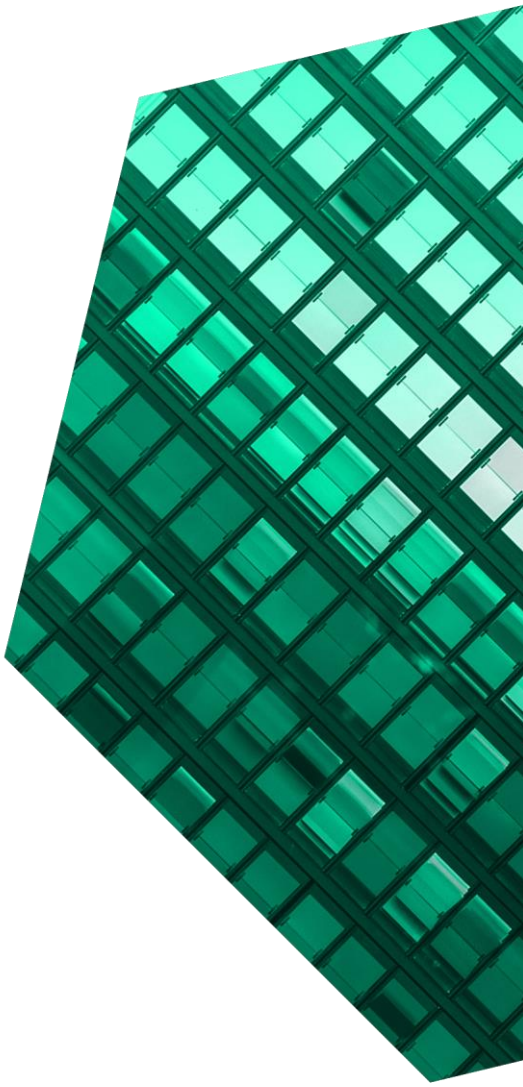
The Total Economic Impact™ Of Microsoft Azure Network Security

Cost Savings And Business Benefits Enabled By Azure Network Security

OCTOBER 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

As organizations move their computing from on-premises to the cloud, they realize that leveraging cloud-native security tools can provide additional cost savings and business benefits to their security infrastructure. Azure network security customers reduced their total cost of ownership of security tools, improved the cost and time-to-value of their development processes through development, security, and operations (DevSecOps), and reduced their risk of a material security breach by 30%.

Azure network security offers a suite of cloud-native security tools to protect Azure workloads while automating network management, implementing DevSecOps practices, and reducing the risk of a material security breach.

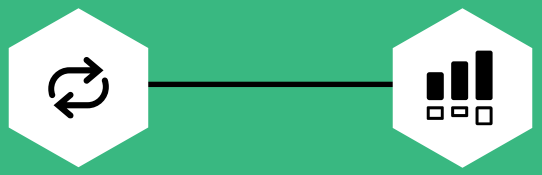
Microsoft commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Azure network security. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Azure network security on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four customers with experience using Azure network security. 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 Azure network security, the interviewees' organizations were utilizing on-premises security tools to protect either on-premises computing environments or nascent cloud workloads. However, the inflexibility and hands-on nature of these tools led to increased time burdens on IT and other inefficiencies that prevented IT professionals from focusing on higher value work.

After the investment in Azure network security, interviewed customers reduced their total cost of ownership related to security infrastructure, established DevSecOps processes, reduced their risk of material security breaches, and reduced the burden on IT to manage networks and upgrades, allowing these teams to focus on more strategic workstreams.

KEY STATISTICS



Return on investment (ROI)
165%

Net present value (NPV)
$1.39M

Development speed acceleration

3x

KEY FINDINGS

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

- **Increased speed of delivering development projects by one month or 67%.** Azure network security enabled organizations to implement

infrastructure-as-code practices, incorporating security directly into application development workflows and speeding development and time-to-market of applications. With the adoption of DevSecOps workflows, security moved to being an enabler of development speed rather than a gate.

- **Reduced total cost of on-premises security tools by 25%.** Organizations reduced their total cost of ownership of on-premises security tools by 25% when protecting 20% of their organization's total computing with Azure network security. Interviewees saved costs directly related to decommissioned on-premises security tools as well as time costs to maintain this infrastructure and from vendor management.
- **Reduced risk of a security breach of 30%.** Azure network security provides automated network security upgrades and improved visibility of the environment. This improves the overall security environment of Azure workloads and reduces the likelihood of experiencing external and internal costs associated with a breach.
- **Improved efficiency of network-related IT work by 73%.** Azure network security improved the efficiency of IT teams delivering network-related work. It reduced firewall management by 80%, security policy management by 15%, and security audit process by 96% without decreasing vulnerabilities.

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

- **Improved hiring and retention.** Owing to its ease of use and enablement of IT teams to do more strategic work, some interviewed customers experienced improved quality of job applicants and improved retention of already hired IT professionals after implementing Azure network security.
- **Microsoft support.** Interviewed customers described working with Microsoft support closely to influence new Azure network security products that would further enhance their security posture and optimize their network-related workstreams.

Costs. Risk-adjusted PV costs include:

- **Azure consumption fees.** Azure consumption fees are based on the number of workloads Azure network security protects. They are typically based on units per hour with a variable

> **"Azure network security is reliable and feature-rich. We're not constantly patching and making updates anymore."**
>
> — VP of applications and infrastructure, education

cost based on network traffic. For the composite organization, total Azure network security fees amounts to under $130,000 annually.

- **Cost of implementation and ongoing management.** Azure network security requires approximately 80 hours of work each for 4 IT FTEs to implement each service. On an ongoing basis, 40 hours per week are needed to manage Azure network security services.

The customer interviews and financial analysis found that a composite organization experiences benefits of $2.23M over three years versus costs of $840.3K, adding up to a net present value (NPV) of $1.39M and an ROI of 165%.

Improved time-to-market of applications

67%

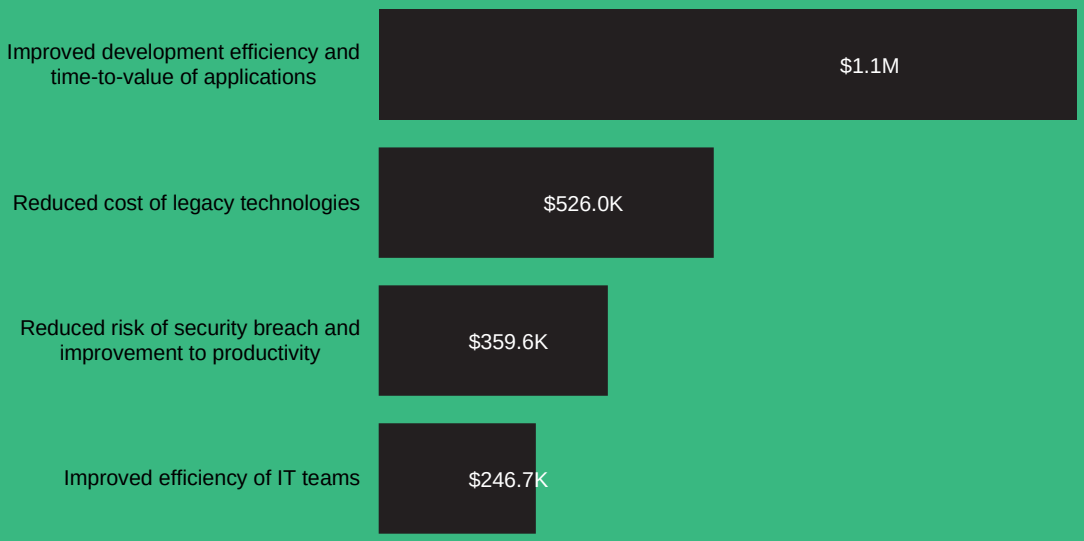
ROI
165%

BENEFITS PV
$2.23M

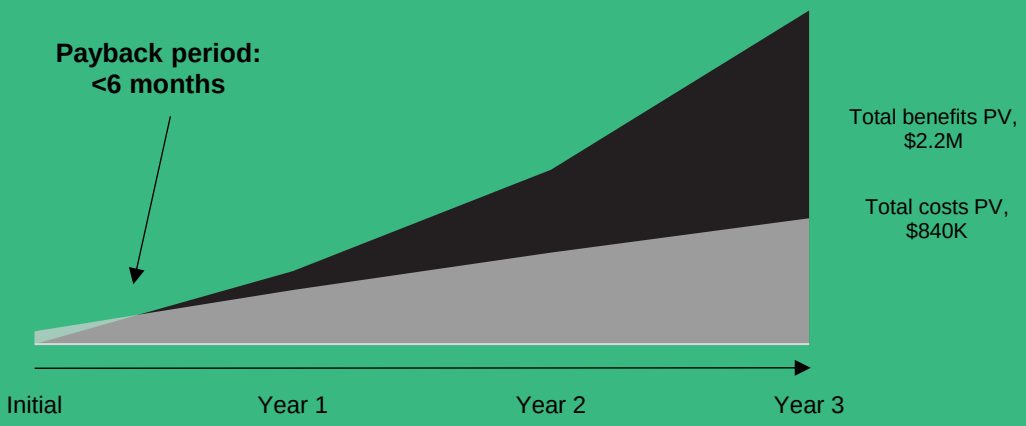
NPV
$1.39M

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 Azure network security.

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

DUE DILIGENCE

Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to Azure network security.

CUSTOMER INTERVIEWS

Interviewed four decision-makers at organizations using Azure network security to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

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

FINANCIAL MODEL FRAMEWORK

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

CASE STUDY

Employed four fundamental elements of TEI in modeling 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 Azure Network Security Customer Journey

Drivers leading to the Azure network security investment

Interviewed Organizations

Industry	Region	Interviewee	Azure network security services
Professional services	EMEA	Senior network analyst	DDoS Protection Azure Firewall Azure Front Door Azure WAF
Education	US	VP of applications and infrastructure	DDoS Protection Azure Firewall Azure WAF
Technology	US	Chief information security officer; chief solutions architect	DDoS Protection Azure WAF
Professional services	US	Enterprise infrastructure architect; assistant director and cloud engineer	DDoS Protection Azure Firewall Azure Front Door Azure WAF

KEY CHALLENGES

Before investing in Azure network security, the interviewees' organizations were either not invested in the cloud or in the early stages of their journey to becoming cloud-first. Those interviewees' organizations who had not yet invested in the cloud ran traditional on-premises security appliances in their data centers to meet their security needs. Interviewees' organizations who had started migrating to the cloud utilized cloud implementations of their on-premises security solutions to protect cloud workloads while also mimicking data center practices for their cloud environments.

The interviewees' organizations struggled with common challenges, including:

- **Inflexibility of on-premises infrastructure.** These prior environments were difficult and expensive when it came to scaling to meet organizational needs. As on-premises computing scaled, organizations would go through the same procurement processes to secure additional security appliances. This incurred a time cost and required organizations to build predictions for growth of computing resources into their security investments. This led to constant overinvestment in security capabilities to ensure adequate protection. Also, this infrastructure could not scale down if organizational needs decreased, resulting in a sunk cost with no risk mitigation benefit.
- **Inefficient security-related workstreams.** Interviewees' organizations faced additional expenses managing their security and undertaking regular workstreams. With physical security appliances on-premises, organizations' teams spent a good amount of their time running manual security-related processes like scripting and patching.
- **Unreliable updates.** Given that the organizations themselves were responsible for management of their on-premises infrastructure, certain workstreams like patching were not completed on schedule. Sometimes, this was due to limited resources being available for patching work and other times it was due to the unreliability of the physical hardware. The regular failure to keep up with updates meant an increased security risk.

“One of the key things has been saving our weekends. We’re no longer spending them implementing change requests or doing software upgrades.”

Senior network analyst, professional services

INVESTMENT OBJECTIVES

The interviewees’ organizations searched for a solution that could:

- Scale up and down easily.
- Automate manual workloads.
- Improve the risk profile of the organization.

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 global business-to-business organization employs 75,000 full-time employees and generates $15 billion in revenue annually. It has recently begun its journey to becoming a cloud-first business. Previously, it regularly invested $1.6 million in security infrastructure for a three-to-five-year term. It experiences an average of 3.1 material security breaches annually, which causes 3.6 hours of lost time to 10% of employees.

Deployment characteristics. The organization has decided to invest in four Azure network security services: Distributed Denial-of-Service (DDoS) Protection, Azure Firewall, Azure Front Door, and Azure Web Application Firewall. The composite migrates 10% of its computing to Azure in Year 1 with an additional 5% moved in the following years for a total of 20% of organizational computing happening in Azure by Year 3.

Key assumptions

- **20% of computing in Azure by Year 3**
- **$1.6 million security-related capital expense**
- **3.1 annual security breaches**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Improved development efficiency and time-to-value of applications	$300,450	$450,675	$600,899	$1,352,024	$1,097,059
Btr	Reduced cost of legacy technologies	$16,848	$124,848	$542,448	$684,144	$526,046
Ctr	Reduced risk of security breach and improvement to productivity	$118,820	$146,336	$173,852	$439,007	$359,574
Dtr	Improved efficiency of IT teams	$99,198	$99,198	$99,198	$297,594	$246,691
	Total benefits (risk-adjusted)	$535,316	$821,056	$1,416,398	$2,772,769	$2,229,370

IMPROVED DEVELOPMENT EFFICIENCY AND TIME-TO-VALUE OF APPLICATIONS

Evidence and data. Interviewed customers described enhanced application development practices after investing in Azure network security. Azure network security services enabled interviewees' organizations to:

- Integrate security and debugging into application development processes.
- Adopt an infrastructure-as-code methodology, managing security changes through a piece of code the security team approved.
- Implement security checklists developers use in the application development process rather than having security teams act as a gate in the development process.
- Create standardized templates with parameterized values that can extend across multiple regions.
- Reduce development delays physical development environments and the associated physical security infrastructure cause.
- Reduce development planning time from over one week to several hours.
- Reduce the time to develop by 50% for some interviewed customers.

> **"We're seeing tremendous speed spinning stuff up in cloud. We have given the application team more reach, where in our on-prem data centers, it was difficult to get access to security appliances with different teams doing different workstreams. With Azure, we're able to use ARM templates."**
>
> *Chief solutions architect, technology*

Modeling and assumptions. For the composite organization, Forrester estimates:

- A prior average application development time of 1.5 months.
- An average development team size of 3 FTEs.

- A fully burdened hourly rate per developer of $100.
- An average annual revenue per development project of $1 million.
- Ten development projects completed in Year 1, 15 projects in Year 2, and 20 projects in Year 3.
- A 10% profit margin.

"We've been able to shift 320 hours monthly of 'business-as-usual' activities like maintaining and managing systems to 'invest' activities like development of applications and new capabilities."

Enterprise infrastructure architect, professional services

Risks. The improvement to development efficiency and time-to-value of developed applications will vary with:

- The average development time per application.
- The average development team size.
- The average rate of pay of developers.
- The average annual revenue of developed applications.
- The number of development projects pursued annually.
- The profit margin on applications.

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

Reduced development time

1 month

Improved Development Efficiency And Time-To-Value Of Applications					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Prior total months to complete a development project	Interviews	1.5	1.5	1.5
A2	New total months to complete a development project	Interviews	0.5	0.5	0.5
A3	Reduction in total project time (months)	A1-A2	1	1	1
A4	Reduction in development hours	2,000/12*A3	167	167	167
A5	Average development team size	Composite	3	3	3
A6	Fully burdened hourly rate per developer	Composite	$100	$100	$100
A7	Productivity recapture rate	Forrester	50%	50%	50%
A8	**Reduced labor costs per project**	**A4*A5*A6*A7**	**$25,050**	**$25,050**	**$25,050**
A9	Average annual revenue per development project	Composite	$1,000,000	$1,000,000	$1,000,000
A10	Average monthly revenue per development project	A9/12	$83,333	$83,333	$83,333
A11	**Additional revenue from improved development time**	**A10*A3**	**$83,333**	**$83,333**	**$83,333**
A12	Development project completed annually	Composite	10	15	20
A13	Profit margin	Composite	10%	10%	10%
At	Improved development efficiency and time-to-value of applications	(A8*A12)+(A11*A12*A13)	$333,833	$500,750	$667,666
	Risk adjustment	↓10%			
Atr	Improved development efficiency and time-to-value of applications (risk-adjusted)		$300,450	$450,675	$600,899
	Three-year total: $1,352,024			**Three-year present value: $1,097,059**	

REDUCED COST OF LEGACY TECHNOLOGIES

Evidence and data. Interviewees shared that as their organizations moved from on-premises computing to cloud computing, their on-premises security appliances were decommissioned in favor of cloud-native security tools like Azure network security. This enabled the interviewees' organizations to avoid the cost of reinvesting in three-to-five-year contracts for their security appliances and additional costs from running more agents and services in the cloud with third-party tools.

"With Azure network security, we don't have to worry about buying a new firewall for a data center. We just spin it up for three weeks and turn it off if we do not need it. It's easy to see where the savings come from when you need to buy less products."

Senior network analyst, professional services

Interviewees also described eliminating IT workstreams related to managing and upgrading security appliances on-premises. The VP of applications and infrastructure from the education industry stated, "We were able to redirect work previously dedicated to configuring load balancers and patching, basically your garden variety care and feeding of these devices to additional cloud deployment, creating a snowballing effect for our cloud migration."

"We were able to more cost-effectively use Azure security to manage our workloads in the cloud and reduced the footprint of additional agents or services for our cloud, which is clearly different than on-prem data centers."

Chief solutions architect, technology

Interviewees also noted that their organizations experienced cost savings related to vendor management. By consolidating security under a single vendor for their cloud workloads, organizations spent less time managing integrations or dealing with finger pointing when something went wrong. As the chief solution architect from the technology industry shared: "We no longer need to manage multiple third parties for integrations. With Azure, integrations are just part of the platform. So, it makes it easy to not only manage vendor relationships but also do overall management of services."

"Before Azure network security, we had an outage where we were managing calls with three vendors: three different IT teams, three systems' support, three sets of account managers. There was a lot of finger pointing and, in the end, the issue was never even resolved. Now, everything is resolved in a matter of hours."

Chief solutions architect, technology

Modeling and assumptions. For the composite organization, Forrester estimates:

- An avoided $1.6 million avoided investment in security-related on-premises infrastructure and associated 15% maintenance fees is realized in Year 3.
- The reallocation of 1 FTE with a fully burdened annual salary of $120,000.
- A total of 320 hours needed for vendor management.
- A fully burdened hourly rate for IT professionals of $60.

Risks. The reduced cost of legacy technologies will vary with:

- The avoided capital expenditure of on-premises security infrastructure.
- The rate of maintenance fees.
- The rate of cloud adoption.

- The number of FTEs reallocated.
- The number of hours dedicated to vendor management.
- The fully burdened rate of IT employees.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $526,046.

Reduced Cost Of Legacy Technologies

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Cost of on-premises security infrastructure and associated maintenance fees	Interviews; Forrester			$2,320,000
B2	Reduction in cost from Azure network security	Composite			20%
B3	**Reduced fees from decommissioned technologies**	**B1*B2**	**$0**	**$0**	**$464,000**
B4	Reallocation of FTEs from infrastructure maintenance work	Interviews		1	1
B5	Annual cost of one IT professional	Composite		$120,000	$120,000
B6	**Reduced cost of maintaining decommissioned technologies**	**B4*B5**	**$0**	**$120,000**	**$120,000**
B7	Prior hours dedicated to vendor management	Interviews	320	320	320
B8	New hours dedicated to vendor management	Interviews	8	8	8
B9	Fully burdened hourly rate for IT employees	Forrester	$60	$60	$60
B10	**Reduced time cost of vendor management from consolidation**	**(B6-B7)*B8**	**$18,720**	**$18,720**	**$18,720**
Bt	Reduced cost of legacy technologies	B3+B6+B10	$18,720	$138,720	$602,720
	Risk adjustment	↓10%			
Btr	Reduced cost of legacy technologies (risk-adjusted)		$16,848	$124,848	$542,448
	Three-year total: $684,144			**Three-year present value: $526,046**	

REDUCED RISK OF SECURITY BREACH AND IMPROVEMENT TO PRODUCTIVITY

Evidence and data. After investing in Azure network security, interviewees reduced exposure to security threats and improved security posture. These improvements stemmed from the following:

- Patching is now automated and Microsoft handles it, eliminating the patching delays that interviewed customers experienced on premises.
- Software is updated and upgraded on time, so that the latest, most protected versions are always running.

- Consolidating security services on Azure provides a centralized risk profile of the environment, enhancing visibility.

"There is no doubt Azure network security improved our security posture. I feel far more comfortable and sleep much better at night having our Azure estate protected by Azure network security as opposed to the combination of what we had on premises."

VP of applications and infrastructure, education

Interviewees' organizations also experienced reduced downtime due to security breaches after deploying Azure network security services. The VP of applications and infrastructure from the education industry stated: "Even though it's in the cloud, these things are not 100%. Despite that, we've experienced only one unplanned outage with regards to Azure over the last two years, while we've had three in that similar timeframe with on-prem and at least a half dozen with [another public cloud platform]."

"The cost of downtime comes down to the core of our business. We can't make money when certain applications are down, so it's business critical."

VP of applications and infrastructure, education

Modeling and assumptions. For the composite organization, Forrester estimates:

- Average annual material security breaches of 3.1.
- Average total internal and external costs of material security breaches of $657,494 per breach.
- The organization is protecting all Azure workloads with Azure network security.
- The addition of Azure network security decreases risk of a security breach by 30% over the prior environment.
- Total downtime per material breach of 3.6 hours.
- This downtime affects 10% of the organization's FTEs.
- An average fully burdened hourly rate of affected employees of $35.
- These employees recapture 25% of their lost productivity as downtime is reduced.

Reduced risk of a security breach

30%

Risks. The reduced risk of a security breach and improvement to productivity will vary with:

- The number and cost of material security breaches.
- The rate of cloud adoption.
- The amount of downtime and affected employees.
- The average employee rate of pay.

- The ability of employees to recapture their productivity lost to downtime.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $359,574.

Reduced Risk Of Security Breach And Improvement To Productivity

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Average annual number of material breaches	Forrester	3.1	3.1	3.1
C2	Average total internal and external costs of a material breach	Forrester	$657,494	$657,494	$657,494
C3	Percentage of organization protected by Azure network security	Interviews	10%	15%	20%
C4	Percentage risk improvement from Azure network security	Interviews	30%	30%	30%
C5	**Reduced risk of a security breach**	**C1*C2*C3*C4**	**$61,147**	**$91,720**	**$122,294**
C6	Prior downtime hours from breach per employee annually	Composite	3.6	3.6	3.6
C7	Number of employees affected	Composite	7,500	7,500	7,500
C8	Average fully burdened hourly rate per employee	Forrester	$35	$35	$35
C9	Productivity recapture rate	Forrester	25%	25%	25%
C10	**Improved productivity from reduced downtime**	**C6*C7*C8*C9*C4**	**$70,875**	**$70,875**	**$70,875**
Ct	Reduced risk of security breach and improvement to productivity	C5+C10	$132,022	$162,595	$193,169
	Risk adjustment	↓10%			
Ctr	Reduced risk of security breach and improvement to productivity (risk-adjusted)		$118,820	$146,336	$173,852
	Three-year total: $439,007			**Three-year present value: $359,574**	

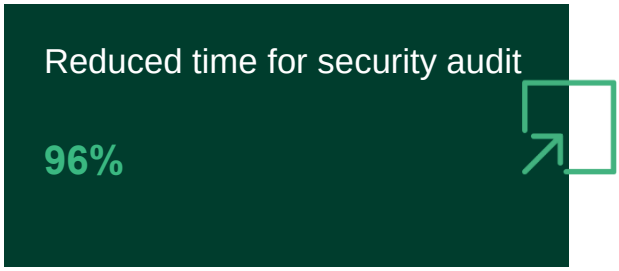
IMPROVED EFFICIENCY OF IT TEAMS

Evidence and data. Lastly, the interviewees reported that Azure network security reduced the time cost of network-related security operations that the Azure platform didn't automate. While patching and upgrading were automated on Azure and application-related security became codified in DevOps practices, organizations described three key areas where network professionals' work was reduced but not eliminated. This included:

"Azure is managing the network, but we do update firewalls. However, because of Azure network security, we can do everything as code. We push changes through as a development organization would."

Chief solutions architect, technology

- Firewall management (85% time savings).
- Security policy management (15% time savings).
- Security audit processes (96% time savings).



Modeling and assumptions. For the composite organization, Forrester estimates:

- Two thousand hours previously needed to manage firewalls is reduced by 80%.
- Three hundred hours previously needed to manage security policy is reduced by 15%.
- Two FTEs save 24 hours each quarter on security audit processes.

Risks. The improved efficiency of IT teams may vary with:

- The prior amount of time spent managing firewalls, security policies, and undergoing security audit processes.
- The rate of pay of affected IT professionals.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $246,691.

Improved Efficiency Of IT Teams

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	IT labor time saved managing firewalls	2,000 hours*80% reduction	1,600	1,600	1,600
D2	IT labor time saved managing policy	300 hours*15% reduction	45	45	45
D3	IT labor time saved on audit process	24 hours*2 FTEs*4 quarters	192	192	192
D4	Hourly cost of IT professional	A10	$60	$60	$60
Dt	Improved efficiency of IT teams	(D1+D2+D3)*D4	$110,220	$110,220	$110,220
	Risk adjustment	↓10%			
Dtr	Improved efficiency of IT teams (risk-adjusted)		$99,198	$99,198	$99,198
	Three-year total: $297,594			**Three-year present value: $246,691**	

UNQUANTIFIED BENEFITS

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

- **Improved hiring and retention.** Some interviewees' organizations leveraged Azure network security and experienced an improvement in the quality of job applicants for open positions. The VP of applications and infrastructure from education stated: "First of all, there has been a significant draw for open positions. Now the market knows that the work is

on Azure, I get much higher-quality candidates. And so, there's definitely a drop that way. Second, the folks I have working on Azure, they're so excited to be working on the technology that it's a significant drop in attrition."

- **Microsoft support.** Regarding Microsoft support, the enterprise infrastructure architect from professional services shared: "We're seeing them take a lot of our ideas back to the product groups. Specifically on networking, we are seeing a lot of the things that we asked for come to market and it's happening exponentially faster."

FLEXIBILITY

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

- **Facilitation of adoption of agile development.** The VP of applications and infrastructure from education stated: "Our migration to Azure was almost perfect from an agile perspective. When we tackled this migration, I felt like we were really enabled from the stability of the environment, from the availability of the tools to integration of those tools. I think it was really quite fantastic."

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	Total Azure consumption fees	$0	$171,917	$171,917	$171,917	$515,750	$427,532
Ftr	Cost of implementation and ongoing management	$84,480	$132,000	$132,000	$132,000	$480,480	$412,744
	Total costs (risk-adjusted)	$84,480	$303,917	$303,917	$303,917	$996,230	$840,276

TOTAL AZURE CONSUMPTION FEES

Evidence and data. Azure network security fees are based on a number of factors, such as the number of workloads protected based on units per hour and a variable cost based on network traffic. For the composite organization, Forrester uses the average spend per Azure network security service for the composite's industry.

Modeling and assumptions. For the composite organization, Forrester estimates:

- Azure DDoS Protections fees of $70,584 annually.
- Azure Firewall fees of $33,948 annually.
- Azure Front Door Service fees of $6,960 annually.
- Azure Web Application Firewall fees of $44,796 annually.

Risks. The total cost from Azure consumption fees will vary with:

- The number of workloads protected and the units per hour consumed on Azure.
- The variable cost of network traffic.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $427,532.

Total Azure Consumption Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Azure DDoS Protections fees			$70,584	$70,584	$70,584
E2	Azure Firewall fees			$33,948	$33,948	$33,948
E3	Azure Front Door Service fees			$6,960	$6,960	$6,960
E4	Azure Web Application Firewall fees			$44,796	$44,796	$44,796
Et	Total Azure consumption fees	E1+E2+E3+E4	$0	$156,288	$156,288	$156,288
	Risk adjustment	↑10%				
Etr	Total Azure consumption fees (risk-adjusted)		$0	$171,917	$171,917	$171,917
	Three-year total: $515,750			**Three-year present value: $427,532**		

COST OF IMPLEMENTATION AND ONGOING MANAGEMENT

Evidence and data. Interviewees described incurring internal implementation and ongoing management time costs for each of the four services deployed. The average deployment for each service required four FTEs to work 80 hours each. For all solutions, interviewees' organizations required 10 FTEs spending 10% of their time on ongoing management.

Modeling and assumptions. For the composite organization, Forrester estimates:

- It takes 4 FTEs 80 hours each per deployed service to implement the four Azure network security services.
- Ten FTEs need to spend 10% of their time managing Azure network security services.
- An average fully burdened hourly rate per IT professional of $60.

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

- The number of Azure network security services deployed.
- The rate of pay of IT professionals.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $412,744.

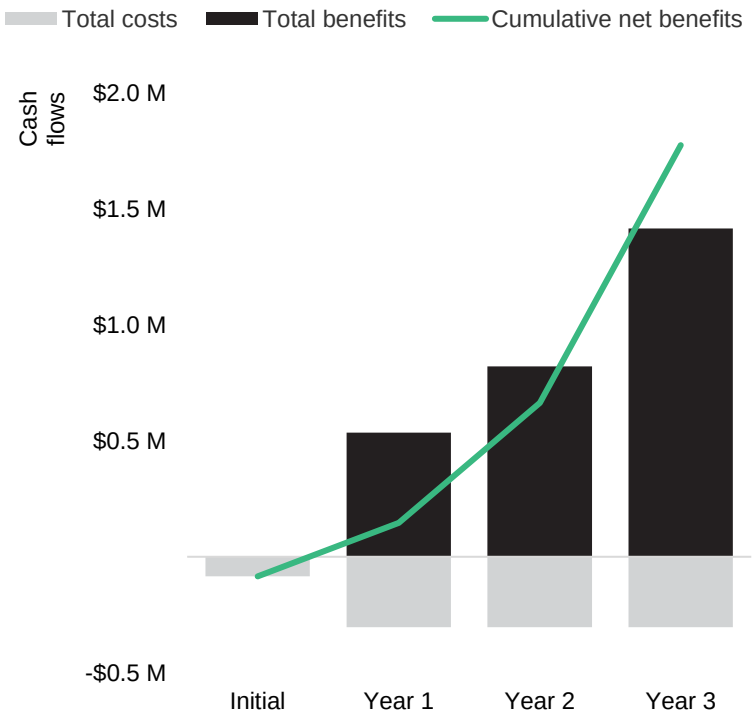
Cost Of Implementation And Ongoing Management

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Total hours to implement per solution	Interviews	1,280			
F2	Total annual hours to manage on an ongoing basis	Interviews		2,000	2,000	2,000
F3	Fully burdened hourly rate for IT professional		$60	$60	$60	$60
Ft	Cost of implementation and ongoing management	Initial: F1*F3 Y1, Y2, and Y3:F2*F3	$76,800	$120,000	$120,000	$120,000
	Risk adjustment	↑10%				
Ftr	Cost of implementation and ongoing management (risk-adjusted)		$84,480	$132,000	$132,000	$132,000
	Three-year total: $480,480			**Three-year present value: $412,744**		

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	($84,480)	($303,917)	($303,917)	($303,917)	($996,230)	($840,276)
Total benefits	$0	$535,316	$821,056	$1,416,398	$2,772,769	$2,229,370
Net benefits	($84,480)	$231,399	$517,139	$1,112,481	$1,776,539	$1,389,094
ROI						165%
Payback period (months)						<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.


FORRESTER®