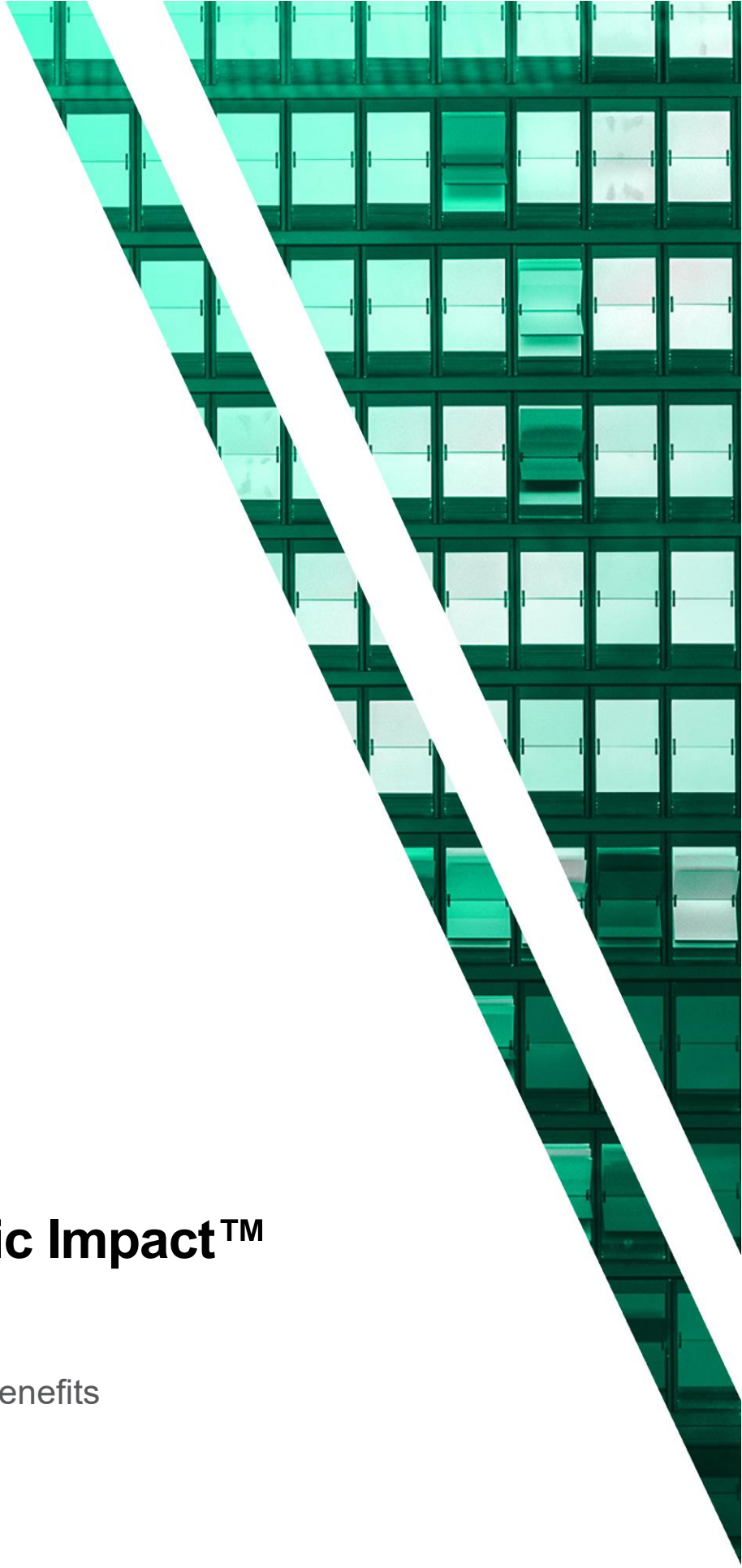
FORRESTER®



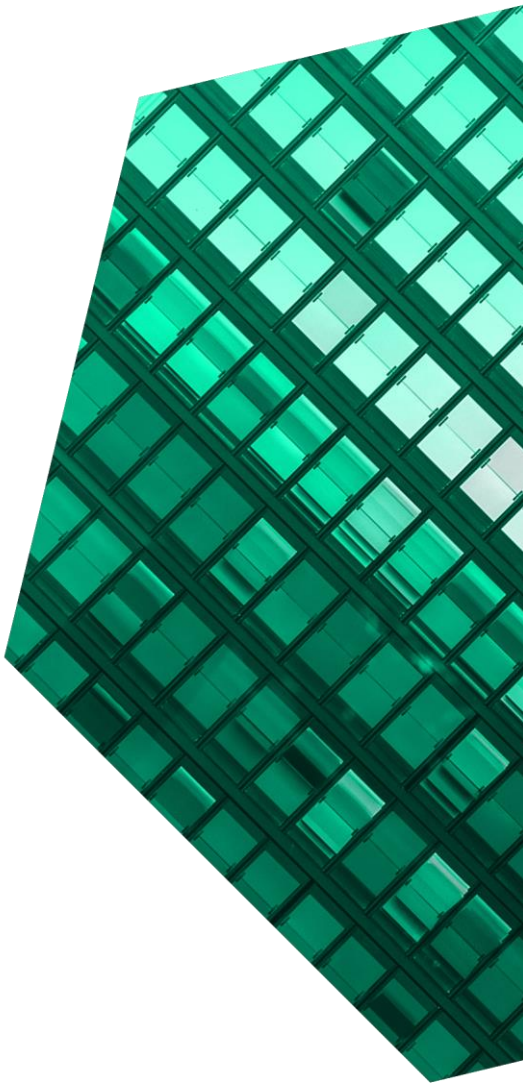
The Total Economic Impact™ Of Tufin

Cost Savings And Business Benefits Enabled By Tufin

MAY 2023

Table Of Contents

Consulting Team: Kara Luk
Nick Ferrif



ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.

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

Executive Summary

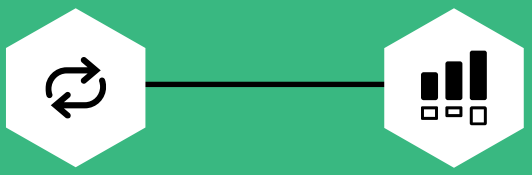
All organizations, large and small, have critical assets to protect, including customer data and differentiating intellectual property that will cause business damage or market setback if stolen.[1] As organizations accelerate DevOps practices and deploy applications faster, security teams must manage network access requests and application connectivity requirements in an efficient and secure manner to meet the business needs of greater agility and productivity.

Tufin is a network security policy management solution that drives business agility and protects against threats by automating security management processes. With Tufin, organizations can efficiently implement network access changes, consistently enforce security policies across network environments, and systematically apply network security policy during provisioning processes. Tufin's security policy automation capabilities decrease the risk of breach and noncompliance, reduce costs, improve productivity for IT teams, and accelerate business value.

Tufin commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Tufin.[2] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Tufin on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five representatives with experience using Tufin. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization with annual revenues of $15 billion, 200 firewalls, and strict compliance requirements.

KEY STATISTICS



Return on investment (ROI)
144%

Net present value (NPV)
$5.21M

Reduction in effort for network change analysis and implementation
94%

Prior to using Tufin, these interviewees noted how their organizations relied on spreadsheets and manual processes to manage security policies and network change processes. Prior approaches left their organizations with burdensome levels of manual work for security and network staff, lack of visibility into vulnerabilities and connectivity errors, and difficulty responding to audit and reporting requests. These limitations led to increased risk of breach and high costs to manage network security and compliance activities.

After the investment in Tufin, the interviewees' organizations automated network security policy management activities, enabling network changes to be analyzed and implemented faster, security policies

to be applied consistently across network environments, connectivity management efficiencies, and easier response to audit and reporting requests. Key results from the investment include reduced risk of breach and noncompliance, security policy management labor savings, audit and reporting efficiencies, and acceleration of application and service provisioning.

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Efficiency improvements of 94% for network change analysis and implementation, 85% for ongoing rule maintenance, and 95% for audit preparation and reporting.** Tufin centralizes and automates network security policy management for the composite organization, improving operational efficiency for security teams on activities including network access evaluation and implementation and rule cleanup. Tufin also enables easier reporting and audit preparedness by documenting adherence to regulations and internal policies and tracking network change history, approvals, and exceptions. The ability to automatically generate security attestation and other requested documentation eliminates the need to manually collect information and organize reports for auditors or other parties, saving security team effort. Over three years, the labor cost savings are worth $5 million.
- **Reduced the risk of breach due to vulnerability by 80%.** Tufin reduces the probability and impact of a successful breach. With automated risk analysis capabilities for requested network changes, the composite organization's security teams can better enforce security policies and compliance requirements. Additionally, Tufin identifies risky or unused rules or network objects for cleanup and decommissioning. Improved risk analysis and rule lifecycle management enable the composite's security teams to reduce attack vectors and improve overall security posture. Over three years, the reduced risk exposure is worth over $3.1 million in avoided breach costs and user downtime for the composite organization.
- **Application connectivity management effort is reduced by 75%.** Tufin enables faster provisioning for applications and services through configuration management capabilities. Better visibility into network topology and security configurations help the composite organization's networks operations personnel and IT analysts identify configuration and security requirements earlier in the provisioning process and with less manual labor, reducing errors and rework that impact time to business value. Over three years, the labor efficiency is worth over $715,000.

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified in this study include:

- **Improved time to value for applications.** SLAs and efforts to implement network changes are significantly reduced, deploying applications faster and accelerating business value delivery.
- **Optimized capacity and usage of security staff.** Automation empowers security staff to handle growing workloads without additional overhead needs. The security team members now focus on higher-value, strategic work over repetitive rule management activities.
- **Reduced third-party audit costs.** Improved reporting capabilities and compliance posture reduce the frequency of third-party audits and associated costs.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Licensing fees.** Licensing costs for Tufin are based on the number of firewall and cloud virtual machine (VM) units. Over three years, the composite organization incurs $3.1 million in licensing costs.
- **Implementation, ongoing management, and training costs.** Over three years, implementation, ongoing management, and training costs total $523,100 for the composite organization.

The representative interviews and financial analysis found that a composite organization experiences benefits of $8.83M over three years versus costs of $3.62M, adding up to a net present value (NPV) of $5.21M and an ROI of 144%.

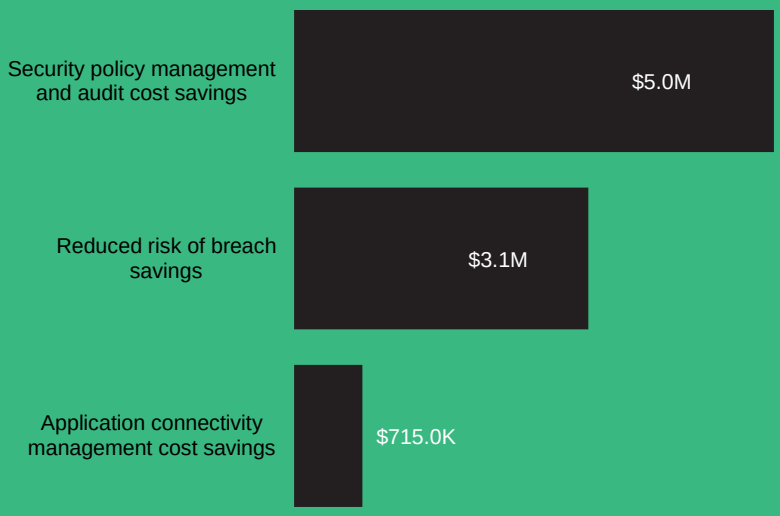
ROI
144%

BENEFITS PV
$8.83M

NPV
$5.21M

PAYBACK
<6 months

Benefits (Three-Year)



“The top benefit we’ve experienced with Tufin is speed, which means that we fit into the company’s agile vision. If they want to deploy any application, all they have to do is access Tufin and make a request. Then, we can implement it in hours instead of weeks.”

— Technical lead for security, financial services

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 Tufin.

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 Tufin can have on an organization.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Tufin and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in Tufin.

Tufin 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.

Tufin provided the customer names for the interviews but did not participate in the interviews.

The Tufin Customer Journey

Drivers leading to the Tufin investment

Interviews				
Role	**Industry**	**Region**	**Employees**	**Revenue**
Director of cybersecurity engineering	Financial services	US HQ Global operations	26,500	$29.3B USD
Network security lead Network security advisor	Financial services	Canada HQ Canadian operations	57,000	$20.3B CAD
Product owner of security orchestration	Telecommunications	EMEA HQ EMEA operations	16,000 – 20,000	€11.4B
Technical lead for security	Financial services	US HQ US operations	650	$329M USD

KEY CHALLENGES

Before adopting Tufin, the interviewees' organizations lacked sophisticated tools for security policy management and network change processes. The organizations relied on tribal knowledge and spreadsheets to define and manage access policies and manual processes to assess and implement network access requests. Dealing with growing, complex network environments, the interviewees' organizations lacked visibility and workflow automation, leading to weak security posture and slow, labor-intensive policy management processes.

The interviewees noted how their organizations struggled with common challenges, including:

- **High SLAs for network access changes due to manual processes.** Interviewees shared that the process of requesting, assessing, designing, and implementing network access changes was highly manual without automated workflows and a centralized view of access and security configurations. Interviewees cited SLAs for access changes ranging from two to four weeks. As a result, security policy management was a bottleneck that slowed down provisioning and application deployment.

> **"Before, we were always focused on getting the proper rules in place and not being able to do anything else. We would have to look into every environment and which firewall goes where, which was difficult due to the complexity of our environment. We would spend a large amount of time researching which enforcement points would need to be implemented and other security rules."**
>
> *Technical lead for security, financial services*

- **Lack of visibility, which increased risk and connectivity errors.** Interviewees noted how limited visibility into their organizations' network topography and security configurations created challenges for connectivity management and adherence to security policies.

The network security lead at a financial services organization shared that IT analysts had to manually analyze paths against firewalls and security policies during the application provisioning process. Lack of visibility often caused errors and connectivity issues, which led to rework and lengthened development time. The network security lead said: "Without a single pane of glass for the network topology, it was difficult for the IT analysts to put in a firewall request and be sure that it would cover the rules need. When they put in a request, it would take a week or so for implementation before they could be allowed to attempt their application or development. And then, if it failed because of a firewall, they would need to wait again."

The technical lead for security at a financial services organization said: "We didn't know if we were violating company policies. We often opened up access more than we should have because we weren't aware of a policy or it was misunderstood. We often thought that a change was okay but didn't know that it actually needed an exception request or an approval."

- **Inconsistent and error-prone manual approaches.** Security engineers had to build and enforce rules based on their knowledge of growingly complex network environments and security policies without the aid of automated workflows. Increasing network complexity and access request volumes paired with a lack of visibility and automation made it difficult to carry out these activities in a consistent and agile manner. The product owner of security orchestration at a telecommunications company said: "We didn't have transparency, so [rule enforcement] depended on the engineer that implemented a change. If the engineer was not well educated, they may not recognize that it is a violation and allow the change."

  The director of cybersecurity engineering at a financial services organization said: "We weren't being consistent because, well, people aren't consistent when they write rules and put stuff in. Many rules were less than ideal, so we'd have to go back and manually rework them to be tighter."

- **Difficulty responding to audits and reporting requests.** Reporting on network change activity, security enforcement, and vulnerabilities created a further burden on security teams and made it difficult to respond to auditors or other parties in a timely manner. For example, the technical lead for security at a financial services organization said: "We could not generate a report in a fast manner. It would take us days to get a report out to the auditors. It was a painful, manual process."

"My company is a financial institute, so we want to get products out as soon as possible. Without an automated tool, it is challenging because everything is manual."

Technical lead for security, financial services

INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that allowed them to:

- Automate network change workflows and policy management and reduce SLAs.
- Strengthen security posture and enable more granular segmentation.
- Gain a centralized view of the network topology and security policy configurations.
- Enable the business to deliver apps and services faster.

WHY TUFIN?

The interviewees noted that they evaluated multiple vendors and chose Tufin due to the maturity of the offering. For example, the director of cybersecurity engineering at a financial organization found Tufin to have superior and flexible workflow design and preferable APIs. Additionally, the technical lead for security at a financial services organization said that Tufin best fit their organization's compliance reporting needs.

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the five interviewees, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The composite organization is a global company that is headquartered in the US with annual revenues of $15 billion and a total of 25,000 employees. The organization has 25 network security engineers and 20 NetOps engineers that work on provisioning. Additionally, the organization must uphold payment card industry (PCI), Service Organization Control Type 2 (SOC 2), and HIPAA compliance.

Deployment characteristics. The composite organization has 200 firewalls, which it uses to enforce network segmentation. Before Tufin, security policies, rule configurations, and network change requests were managed through spreadsheets, providing lack of sophisticated visibility and leading to manual workflows. The composite adopts Tufin to improve enforcement of security policies and compliance requirements; manage more granular levels of segmentation; improve visibility and audit readiness; and automate network change and rule management processes.

"The main drivers were to increase automation and visibility into the network and firewall topology. Ultimately, we wanted to accelerate the delivery of firewall requests. We wanted to deliver faster."

Network security lead, financial services

Key Assumptions

- **$15 billion dollars in annual revenue**
- **25 network security engineers**
- **20 NetOps engineers**
- **PCI, SOC2, and HIPAA compliance requirements**
- **200 firewalls**

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	Security policy management and audit cost savings	$2,023,789	$2,023,789	$2,023,789	$6,071,366	$5,032,863
Btr	Reduced risk of breach savings	$1,240,775	$1,240,775	$1,240,775	$3,722,325	$3,085,623
Ctr	Application connectivity management cost savings	$287,508	$287,508	$287,508	$862,524	$714,990
	Total benefits (risk-adjusted)	$3,552,072	$3,552,072	$3,552,072	$10,656,215	$8,833,476

SECURITY POLICY MANAGEMENT AND AUDIT COST SAVINGS

Evidence and data. Interviewees noted how Tufin centralized and automated network security policy management processes, improving operational efficiency for security teams around activities including network change evaluation and implementation and rule cleanup. By shifting these activities to automated workflows, the security teams reallocated resources to focus on higher-value, strategic work. Interviewees also highlighted that Tufin enabled easier reporting and audit preparedness. Tufin documented adherence to regulations and internal policies and tracked change history, approvals, and exceptions, eliminating the need to collect information and organize reports for auditors or other parties and saving security team effort.

- The interviewees highlighted how time to implement access changes or rule modifications for connectivity was significantly reduced with the move to Tufin.

  The director of cybersecurity engineering at a financial services organization shared that Tufin automated risk analysis and path design processes for requested access changes, which was previously executed manually. As a result, the time to implement access changes was reduced from 2 hours for typical changes and up to 2.5 days for more complex situations, down to 30 minutes. Similarly, the network security lead at a financial services organization noted that it took 2 to 3 hours less to evaluate and implement changes, saving significant time across the 600 requests received per month.

- The product owner of security orchestration at a telecommunications organization shared that it would have been difficult to handle its security requirements without Tufin. Through leveraging

> **"We don't have to write the code. We don't have to have it approved by another team member, and we don't have to schedule a change itself because provisioning has been taught and implemented into Tufin."**
>
> *Network security lead, financial services*

risk analysis and target selection capabilities, the organization automatically assessed proposed changes against its unified security policy and design secure network paths, reducing the time to implement a change from two weeks to 15 minutes. They said: "The USP and security policy check are beneficial. Additionally, the automated target selection is aware of the full topology of our network and can suggest where the firewall rules or enforcement points must be implemented."

- Interviewees also shared that Tufin drove efficiencies around ongoing rule management and cleanup. The technical lead for security at a financial services organization shared that Tufin detected and reported on unused or overly permissive rules enabling risky rules to be more easily identified and submitted for cleanup or decommissioning. Similarly, the director of cybersecurity engineering in financial services noted that Tufin's data was instrumental in helping to cleanup their rule base. They said: "We've got a team of five people, who used to be a rules-writing team. Now, they're focusing on cleanup activities. They take the data out of Tufin and marry it with our own list of servers and server owners to basically recraft the rules."
- The technical lead for security at a financial services organization shared that it took days of effort for security engineers to generate reports for auditors. With Tufin, their organization could leverage a central console for monitoring and documenting compliance with industry regulations and internal policies across its network. Additionally, Tufin provided an audit trail to track and report on change history. They said: "Instead of having to go through the entire environment and extracting a rule to provide compliance to an auditor, we can quickly generate a report. There's an audit trail as well to see which engineer is doing what and whether we have a properly documented chance process in place."
- Similarly, the head of cybersecurity engineering at a financial services organization utilized Tufin to respond to audit requests, reducing over 40 hours of manual effort for each audit down to 20 to 30 minutes. They shared: "We used to have one person spend a week of their life, twice a year producing audit evidence for compliance. Now, Tufin auto-collects those reports and we provide it to the auditors. It's moved from 40-plus hours of collecting data down to an auto-report that takes 20 to 30 minutes to produce."
- The director of cybersecurity engineering at a financial services organization also highlighted that Tufin aided their team in investigating and reporting on vulnerabilities, reducing the effort per vulnerability from a range of 8 to 12 hours to 45 minutes: "We would have to go through two different gateways and built a report with Splunk. I would say it probably would have taken us 8 if not 12 hours to collate all of that and figure out the flows and configuration. Reducing a whole day or 12 hours down to less than an hour is great."

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

- The network security team receives 5,000 network access change requests each year.
- Prior to Tufin, it took 4 hours for a network security engineer to analyze, design, and implement each access change. With Tufin, this

Reduction in ongoing rule maintenance effort

85%

process is completed in 15 minutes, a 94% reduction in effort.

- The hourly fully burdened salary of a network security engineer is $88.
- Each of the composite organization's 25 network security engineers also spend 10% of their time on ongoing rule maintenance.
- With Tufin, efforts for ongoing rule maintenance are reduced by 85% through automation.
- The full-time equivalent of half a security engineer works on reporting to auditors or other parties each year.
- Tufin enables a 95% efficiency gain for audit preparation and reporting activities.

Risks. Forrester understands that these results may not be representative of all experiences and may vary depending on the following factors:

- The number of network access changes.
- The efficiency of implementing network access changes in the prior environment.
- Network engineer salary.
- The volume of rule review backlogs.
- Integration with service management or vulnerability scanner tools.
- An organization's compliance requirements
- The frequency and complexity of audits or other events that require reporting related to security policies or firewalls.

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

"With Tufin, we can keep track of rules and see when they haven't been hit for three months so we can then instruct a junior engineer to submit a cleanup or rule decommission. It's all tracked within the system so we know what's been disabled and what's still active. It's helped us to cleanup the firewall rules."

Technical lead for security, financial services

"We were spending days of multiple engineers' time trying to prove to auditors that we had policies in place. With Tufin, we can generate reports in minutes or a few hours if it's a large amount of data."

Technical lead for security, financial services

Security Policy Management And Audit Cost Savings					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Number of network changes	Composite	5,000	5,000	5,000
A2	Hours per network change prior to Tufin	Interviews	4	4	4
A3	Hours per network change with Tufin	Interviews	0.25	0.25	0.25
A4	Reduction in effort for network changes (rounded)	(A2-A3)/A2	94%	94%	94%
A5	Hourly network security engineer fully burdened salary	TEI Standard	$88	$88	$88
A6	Subtotal: Network change cost savings	A1*A2*A4*A5	$1,654,400	$1,654,400	$1,654,400
A7	Number of network security engineers	Composite	25	25	25
A8	Percentage of time spent on ongoing rule maintenance	Interviews	10%	10%	10%
A9	Reduction in effort for ongoing rule maintenance	Interviews	85%	85%	85%
A10	Subtotal: Rule maintenance cost savings	2080 hours*A5*A7*A8*A9	$388,960	$388,960	$388,960
A11	Network security engineer FTEs working on audit preparation and reporting	Interviews	0.5	0.5	0.5
A12	Audit preparation and reporting efficiency gain	Interviews	95%	95%	95%
A13	Subtotal: Audit preparation and reporting cost savings	2080*A5*A11*A8	$86,944	$86,944	$86,944
At	Security policy management and audit cost savings	A6+A10+A13	$2,130,304	$2,130,304	$2,130,304
	Risk adjustment	↓5%			
Atr	Security policy management and audit cost savings (risk-adjusted)		$2,023,789	$2,023,789	$2,023,789
	Three-year total: $6,071,366		**Three-year present value: $5,032,863**		

REDUCED RISK OF BREACH SAVINGS

Evidence and data. Interviewees shared that Tufin reduced the probability and impact of a successful breach. With automated risk analysis capabilities, security teams gained visibility into requested network changes and their impact on security posture, improving their ability to uphold corporate security policies and compliance requirements. Additionally, Tufin provided a means to identify risky and unused rules or network objects for cleanup and decommissioning. With better capabilities to manage risk analysis and rule lifecycle management, the organizations reduced attack vectors and improved overall security posture.

- The director of cybersecurity engineering at a financial services organization highlighted how Tufin helped their organization visualize where risks were and provided greater control over the network change process. Tufin utilized network traffic data to identify gaps in segmentation and security violations, illuminating opportunities to strengthen security policies and remove attack vectors. For example, Tufin identified ports that were vulnerable to threats like ransomware, enabling them to be shut down. Tufin also flagged requested network access changes that violated security policies, reducing the chance of implementing access changes that could impact risk posture.
- Similarly, the product owner of security orchestration at a telecommunications organization shared that Tufin enforced their organization's global security policy, strengthened security rules, and enabled proper segmentation. They said: "We are now able to enforce our unified security policy and truly have full transparency. To mitigate risk, we have a really complex rule set for microsegmentation, which we would not be able to manage without the proper tools like Tufin."
- The technical lead for security at a financial services organization shared that their team leveraged Tufin's vulnerability management module and risk analysis capabilities. The vulnerability mitigation tool identified high-risk vulnerabilities based on risk scores and network insights, cleaning up highly permissive rules and reducing exposure to risk. Additionally, their organization gained better visibility and control over the network change process by automating risk analysis. They said: "We've gained much more visibility into the firewall rule set and what we are granting access for. If a request shows up that violates company policy, we can quickly

"Tufin shows us who has access to what and what rules we're putting in place. We have definition of zones and what should and shouldn't be going between them. And Tufin tells us if we are in compliance with it or not. It basically goes through and shows that we're enforcing our standards and compliance through these gates."

Director of cybersecurity engineering, financial services

Reduction in risk of breach due to vulnerability

80%

reject it and request for them to go through a secure protocol. We are not opening up any unnecessary requests which helps reduce our attack surface."

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

- The average number of breaches experienced annually is 2.5, potentially costing $654,846 annually on average.[3] These costs include response and remediation costs, notification costs to affected parties, regulatory fines, customer compensation, customer lawsuits and punitive damages, audit and security compliance costs, lost revenue, the cost to rebuild brand equity, and the cost to acquire new customers.
- Sixty percent of breaches stem from unpatched vulnerabilities.[4]
- With Tufin, the risk of breach is reduced by 80% due to improved vulnerability management.
- Ninety percent of the composite organization utilizes internal systems to perform work.
- The hourly fully burdened cost of an internal business user is $52.
- Each breach impacts 12% of internal users causing 4 hours of downtime per year.

Risks. Forrester understands that these results may not be representative of all experiences and may vary depending on the following factors:

- The frequency and cost of a data breach.
- The duration of outages due to a breach.
- Security posture prior to Tufin.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $3.1 million.

"Tufin has helped with the work that we've done on rules that were too wide. The automatic policy generator tracked the traffic that was going on the rule helping us to put a stricter rule on it instead, reducing the attack surface."

Network security advisor, financial services

Reduced Risk Of Breach Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Average number of breaches per year	Forrester research	2.5	2.5	2.5
B2	Average potential cost of breach, excluding internal user downtime	Forrester research	$654,846	$654,846	$654,846
B3	Percentage of unpatched vulnerabilities that cause breach	Industry research	60%	60%	60%
B4	Reduced risk of breach with Tufin due to improved vulnerability management	Interviews	80%	80%	80%
B5	Avoided costs of remediation, customer resolution, fines, brand rebuild, and all other external-facing costs (rounded)	B1*B3*B2*B4	$785,815	$785,815	$785,815
B6	Number of internal business users	Composite	22,500	22,500	22,500
B7	Hourly business user fully burdened salary	TEI standard	$52	$52	$52
B8	Hours of diminished internal user productivity hours per breach	Forrester research	4	4	4
B9	Average percentage of employees impacted per breach	TEI standard	12%	12%	12%
B10	Cost of reduced internal productivity	B1*B3*B4*B6*B7*B8*B9	$673,920	$673,920	$673,920
Bt	Reduced risk of breach savings	B5+B10	$1,459,735	$1,459,735	$1,459,735
	Risk adjustment	↓15%			
Btr	Reduced risk of breach savings (risk-adjusted)		$1,240,775	$1,240,775	$1,240,775
	Three-year total: $3,722,325		**Three-year present value: $3,085,623**		

APPLICATION CONNECTIVITY MANAGEMENT COST SAVINGS

Evidence and data. Interviewees noted that Tufin enabled faster provisioning for applications and services by driving configuration management efficiencies. With better visibility into network topology and security configurations, network operations personnel and IT analysts could identify configuration requirements earlier in the provisioning process and with less manual labor, reducing errors and rework that had previously impacted time to business value.

- The network security lead at a financial services organization noted that Tufin helped IT analysts conduct path analysis to identify network flows that needed to be opened for their applications, saving time and reducing connectivity issues. They said: “For the IT analysts that are making firewall change requests, they have access to the path analysis [through Tufin]. They can check if the path is open or if it goes through three firewalls and one is blocked, so they will need to put in a request for the firewall. If they do not check that and put in a standard access request, the application or development may fail because of a firewall and they’ll need to wait.”
- The product owner of security orchestration at a telecommunications company highlighted that automating configuration processes with Tufin increased speed and quality during application provisioning. With Tufin, business application owners could quickly visualize and identify connectivity requirements, reducing work for connectivity engineers who were tasked with manually doing it before. For example, they shared, “When an application owner adds additional VMs in a group, Tufin can automatically detect that it’s a new IP address and there’s no firewall rules available for it and automatically start a ticket in Tufin.”

> **“In the past, connectivity engineers would have to fulfill all of the connectivity information for the rulesets. But now, the application owners can directly log in to Tufin, find the application, and automate all of the objects in it. That means they can create their own connection and start the change workflow. We do not need security engineers to set it up. The business owners can do it on their own.”**
>
> *Product owner of security orchestration, telecommunications*

- The director of cybersecurity engineering at a financial services organization shared that their network engineers used Tufin as a tool to route infrastructure for new networks, saving over 40 hours for each project. They said: “Having Tufin be able to report holistically on routers, switches, load balancers, and firewalls allows network engineers to understand what a network would look like and how to route it. It saves us major headaches and time because trying to draw a map of it manually wouldn’t work. Instead, we can use a tool that can sit there and plot the actual course.”

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

- The organization has 20 network operations engineers that spend 10% of their time on connectivity management.

- With Tufin, the engineers reduce connectivity management effort by 75%
- The hourly fully burdened cost of a network operations engineer is $97

Risks. Forrester understands that these results may not be representative of all experiences and may vary depending on the following factors:

- The number of network engineers and time spent on connectivity management.
- The fully burdened cost of network engineer resources.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $715,000.

Application Connectivity Management Cost Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	NetOps engineers	Composite	20	20	20
C2	Percentage of time spent on application connectivity management	Assumption	10%	10%	10%
C3	Application connectivity management time savings with Tufin	Interviews	75%	75%	75%
C4	Hourly NetOps engineer fully burdened salary	TEI Standard	$97	$97	$97
Ct	Application connectivity management cost savings	2,080 hours*C1*C2*C3*C4	$302,640	$302,640	$302,640
	Risk adjustment	↓5%			
Ctr	Application connectivity management cost savings (risk-adjusted)		$287,508	$287,508	$287,508
	Three-year total: $862,524		**Three-year present value: $714,990**		

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Improved time to value for applications.** Interviewees noted that they significantly reduced effort and SLAs for implementing network changes, enabling their organizations to deploy applications or services faster and accelerate delivery of business value. For example, the director of cybersecurity engineering at a financial services organization reduced their SLA from seven to four days. Similarly, the technical lead for security at a financial services organization reduced SLAs from weeks down to days: "Before Tufin, firewall implementations were taking weeks to a month. Now with Tufin, I can deploy it in minutes as soon as the request is received and we can help the company deploy applications faster."
- **Optimized capacity and usage of security staff.** Interviewees also shared that automation enabled their organizations to effectively handle growing workloads without needing to add additional staff and security team members could focus on more strategic work. The product owner for security orchestration at a financial services organization noted that their organizations would have needed to hire eight to ten additional FTEs to manage its security requirements and policies without the automation provided by Tufin. The technical lead for security at a financial services organization highlighted that Tufin enabled their organization to shift security policy management activities to junior security resources, enabling senior team members to focus on larger strategic projects. Additionally, the director of cybersecurity engineering at a financial services organization said that staff could refocus on analysis work instead of rule writing.
- **Reduced third-party audit costs.** The technical lead for security at a financial services organization shared that Tufin reduced third-party auditor costs. With better reporting capabilities and improved compliance posture, their organization could more easily provide information to auditors and the frequency of third-party audit requests was reduced, decreasing associated costs by 50%.

"We can refocus staff on what their job really is: posture analysis, attack vectors, efficiency, and flow. It's allowed our staff to move from very low base rule writing up to a kind of engineering level of analysis, which is higher level and much more enjoyable."

Director of cybersecurity engineering, financial services

"We can deploy the applications more quickly to the customers and they will work on all of the systems and buildup will be faster. We have a clear process, transparency on what's going on, and can verify quality when something goes wrong."

Product owner of security orchestration, telecommunications

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Tufin and later realize additional uses and business opportunities, including additional value through integrations. Several interviewees had either integrated or were in the process of integrating Tufin with tools such as IT service management (ITSM) solutions or intelligence portals to drive additional use cases. For example, the technical lead for security at a financial services organization said, “We are working on getting Tufin integrated with [our service management tool], so we can keep track of how many changes there are and management can execute the approval workflows in there and be able to track the process.”

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**
Dtr	Licensing fees	$0	$1,244,880	$1,244,880	$1,244,880	$3,734,640	$3,095,832
Etr	Implementation, ongoing management, and training fees	$271,463	$101,201	$101,201	$101,201	$575,066	$523,135
	Total costs (risk-adjusted)	$271,463	$1,346,081	$1,346,081	$1,346,081	$4,309,706	$3,618,967

LICENSING FEES

Evidence and data. Licensing costs for Tufin were based on the number of firewall and cloud VM units. Interviewees noted that their organizations utilized Tufin's SecureTrack+ and SecureChange+ solutions.

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

- The composite organization has licensing fees of $1,185,600.
- Pricing may vary. Contact a Tufin representative for additional details.

Risks. Forrester understands that these results may not be representative of all experiences and may vary depending on the following factors:

- An organization's volume of firewalls and cloud VMs.
- Pricing variables, such as the subscription tier chosen, discount rates, partner and distributor markups.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $3.1 million.

Licensing Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Tufin licensing fees	Interviews	$0	$1,185,600	$1,185,600	$1,185,600
Dt	Licensing fees	D1	$0	$1,185,600	$1,185,600	$1,185,600
	Risk adjustment	↑5%				
Dtr	Licensing fees (risk-adjusted)		$0	$1,244,880	$1,244,880	$1,244,880
Three-year total: $3,734,640				**Three-year present value: $3,095,832**		

IMPLEMENTATION, ONGOING MANAGEMENT, AND TRAINING FEES

Evidence and data. The interviewees' organizations incurred costs associated with implementation, ongoing management, and training:

- Interviewees cited implementation timelines ranging from two months to over a year and involving two to six security and network engineers who typically dedicated half of their time during the implementation period.
- Interviewees also noted that they incurred professional services costs during the implementation. For example, the technical lead for security at a financial services organization shared: "A prerequisite for the Tufin deployment was to get the entire infrastructure topology. You need to find every router and every firewall that you know of and put it in Tufin and define the zones depending on the USP. We required professional services to carve this out for us in the beginning."
- Interviewees noted that ongoing management requirements were simple, involving half of a security FTE.
- The network security lead at a financial services organization noted that staff on the firewall team received a few days of internal training on Tufin.

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

- A six-month implementation involving four network security engineer resources dedicating 50% of their work hours.
- $50,000 in professional services costs
- Half of a network security engineer FTE is dedicated to ongoing management
- All 25 network security engineers participate in 12 hours of training in the initial period. Each subsequent year, five new network security engineers participate in the training, accounting for turnover.
- The annual fully burdened cost of a network security engineer is $185,250.

Risks. Forrester understands that these results may not be representative of all experiences and may vary depending on the following factors:

- Implementation requirements and the timeline.
- The labor costs of implementation resources and professional services.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $523,100.

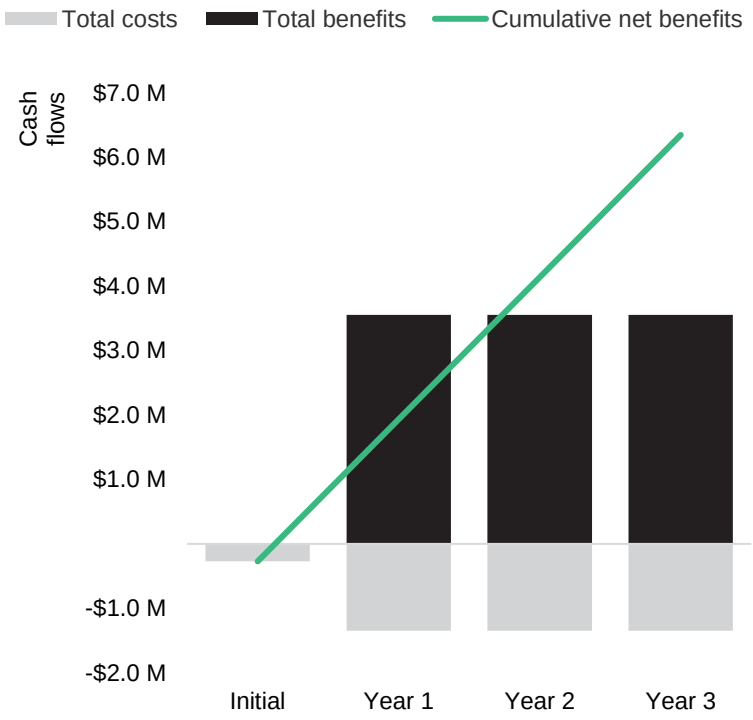
Implementation, Ongoing Management, And Training Fees

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Months to implement Tufin	Interviews	6			
E2	Number of network security engineer resources dedicated to implementation	Interviews	4			
E3	Percent of workload dedicated to implementation	Interviews	50%			
E4	Annual network security engineer fully burdened salary	TEI Standard	$182,250	$182,250	$182,250	$182,250
E5	Professional services costs	Interviews	$50,000			
E6	Subtotal: Implementation costs	E1*E2*E3*E4/12+E5	$232,250			
E7	Number of network security engineer FTEs dedicated to ongoing management	Interviews		0.5	0.5	0.5
E8	Subtotal: Ongoing management costs	E4*E7		$91,125	$91,125	$91,125
E9	Number of network security engineers participating in training	Interviews	25	5	5	5
E10	Hours of training	Interviews	12	12	12	12
E11	Subtotal: training costs (rounded)	E4/2080*E9*E10	$26,286	$5,257	$5,257	$5,257
Et	Implementation, ongoing management, and training fees	E6+E8+E11	$258,536	$96,382	$96,382	$96,382
	Risk adjustment	↑5%				
Etr	Implementation, ongoing management, and training fees (risk-adjusted)		$271,463	$101,201	$101,201	$101,201
	Three-year total: $575,066			**Three-year present value: $523,135**		

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	($271,463)	($1,346,081)	($1,346,081)	($1,346,081)	($4,309,706)	($3,618,967)
Total benefits	$0	$3,552,072	$3,552,072	$3,552,072	$10,656,215	$8,833,476
Net benefits	($271,463)	$2,205,990	$2,205,991	$2,205,991	$6,346,509	$5,214,509
ROI						144%
Payback period (months)						<6

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: “The Forrester Tech Tide™: Zero Trust Threat Prevention, Q4 2022,” Forrester Research, Inc., October 21, 2022.

[2] 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.

[3] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021. Forrester Consulting conducted an online survey of 351 cybersecurity leaders at global enterprises in the US, the UK, Canada, Germany, and Australia. Survey participants included managers, directors, VPs, and C-level executives who are responsible for cybersecurity decision-making, operations, and reporting. Questions provided to the participants sought to evaluate leaders’ cybersecurity strategies and any breaches that have occurred within their organizations. Respondents opted into the survey via a third-party research panel, which fielded the survey on behalf of Forrester in November 2020.

[4] Source: “Costs and Consequences of Gaps in Vulnerability Response,” Ponemon Institute, 2019.


FORRESTER®