A Forrester Total Economic Impact™ Study Prepared For F5 Networks

The Total Economic Impact Of F5 Networks' BIG-IP Security Solutions

Project Director: Dean Davison

August 2013

FORRESTER®

Headquarters | Forrester Research, Inc.
60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617.613.6000 | www.forrester.com

Forrester Consulting
Making Leaders Successful Every Day

TABLE OF CONTENTS

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

Executive Summary

In May 2013, F5 Networks commissioned Forrester Consulting to examine the total economic impact and potential return on investment (ROI) enterprises may realize by deploying its BIG-IP security solutions. To understand the impact of using F5 for intelligent network security, Forrester conducted interviews with four existing customers of the BIG-IP products from F5 and compiled the results into a composite case study for a $2 billion company with 12,000 employees that manufactures and distributes consumer products — referred to as a consumer products manufacturing company (CPMC). See Appendix A for a description of the composite organization.

F5 Networks provides devices that deliver intelligent network security — and secure the activities of users — by monitoring end-to-end network traffic rather than managing security for each application or device. Using a networkwide architecture allows F5 tools to protect the user experience regardless of the type of device being used. In other words, BIG-IP enables users to bring-your-own-device (BYOD).

A CPMC Secures Users On Any Device, Anywhere, With BIG-IP Security Solutions

The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of F5 BIG-IP security solutions on their organizations. Forrester found that the CPMC experienced a risk-adjusted ROI of 537% with the costs and benefits shown in Table 1.

Among the benefits realized by F5 customers is the ability to provide security as users access data and applications through a wide range of devices — especially tablets and smartphones. F5 secures the network rather than individual devices or applications and thus monitors the entire range of users' activities, including the device being used, the application being accessed, and the data that is being transferred. As a result, users are secure from inception through termination, and security professionals are able to refocus on detecting and preventing other security vulnerabilities.

Table 1
Three-Year Risk-Adjusted ROI

ROI	Payback period	Total benefits (present value)	Total costs (present value)	Net present value
537%	4.6 months	$2,056,806	($323,123)	$1,733,683

Source: Forrester Research, Inc.

- **Benefits.** The CPMC experienced the following benefits:
    - **Eliminated standalone firewalls.** By managing the security of the entire network with F5, the CPMC no longer requires some standalone firewalls — network or application — on which it previously relied. The ability to eliminate 53 firewalls over three years provides $190,800 in savings.

- **Supported and secured the migration to BYOD.** The value to the CPMC of securing the migration of users on any kind of device with F5 is valued at $614,100, based on the boost in productivity, as business users are able to use a wider range of devices.
- **Avoided site outages even during intense DDoS attacks.** F5 provides the CPMC with the ability to filter legitimate site traffic from distributed denial of service (DDoS) traffic on critical shopping days — Black Friday — resulting in $477,692 of profit from sales that would be lost otherwise.
- **Avoided server remediation by proactively patching security vulnerabilities.** F5's products include a platform called iRules for applying custom code as network security rules — i.e., virtual patching. The ability to close security risks from third-party products immediately rather than waiting for patches from software vendors saves the CPMC more than $177,561 in costs that it would incur for server remediation.
- **Avoided customer triage by proactively patching security vulnerabilities.** By using iRules to virtually patch security holes immediately, the CPMC eliminates breaches that compromise customer data. As a result, the CPMC avoids more than $1 million in costs for communicating with customers and providing credit protection services.

- **Costs.** The CPMC experienced the following costs:
  - **Licensing F5 Networks' BIG-IP products.** The cost for the CPMC to license and maintain two BIG-IP Local Traffic Managers and one Edge Gateway is a total of $462,000 over three years.
  - **Training for security professionals.** During the first year, the CPMC purchases on-site training for the entire security team. In addition, the eight security professionals attend product-specific training courses. The total training investment is $127,000.

Disclosures

The reader should be aware of the following:

- The study is commissioned by F5 Networks and delivered by the Forrester Consulting group.
- Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers should use their own estimates within the framework provided in the report to determine the appropriateness of an investment in F5 Networks BIG-IP security solutions.
- F5 Networks 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.
- The customer names for the interviews were provided by F5 Networks.

TEI Framework And Methodology

Introduction

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering implementing F5 Networks solutions. The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision.

Approach And Methodology

Forrester took a multistep approach to evaluate the direct and indirect financial impact that F5 Networks can have on an organization (see Figure 1). Specifically, Forrester:

- Interviewed F5 Networks marketing/sales/consultants personnel and Forrester analysts to gather data relative to F5 products and the marketplace for application security.
- Interviewed four organizations currently using F5 Networks products to obtain data with respect to costs, benefits, and risks.
- Designed a composite organization based on characteristics of the interviewed organizations (see Appendix A).
- Constructed a financial model representative of the interviews using the TEI methodology. The financial model is populated with the cost and benefit data obtained from the interviews as applied to the composite organization.

Figure 1
TEI Approach

Source: Forrester Research, Inc.

Forrester employed four fundamental elements of TEI in modeling F5 Networks solutions:

1. Costs.
2. Benefits to the entire organization.
3. Flexibility.
4. Risk.

Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves the purpose of providing a complete picture of the total economic impact of purchase decisions. Please see Appendix B for additional information on the TEI methodology.

Analysis

Interview Highlights

Forrester conducted a total of four interviews for this study, involving executives from the following companies:

1. **A producer of consumer products.** The company maintains individual websites for dozens of brands and therefore needs security tools that allows it to manage the sites in aggregate rather than individually, giving the company benefits such as economies of scale in managing servers and load balancing for Internet traffic.

2. **A specialty products retailer.** The company supplies specialty electronics to businesses and consumers. Although the company built its reputation through brick-and-mortar stores, its online sales are now several times larger than in-store sales. The retailer is concerned with providing the same quality of high-touch, high-quality shopping experience online as in its stores.

3. **A community college.** The college has dozens of buildings on its campus and provides hundreds of applications for college students, staff, and the surrounding community. The college had a goal for any user to access any application from any location on-campus using any device — making the college an early and aggressive adopter of BYOD. As a result, the college needed security that provides end-to-end security for users anytime, anywhere, and on any device.

4. **A regional medical center.** The center includes a large hospital, several associated clinics, and thousands of highly specialized doctors. The medical center is consolidating patient's medical records and providing access to physicians, specialists, and staff to patient records on mobile devices. To comply with the Health Insurance Portability and Accountability Act (HIPAA) requirements, the medical center must secure patient privacy while providing access in an environment where performance literally saves lives.

Although the four companies span various industries, they faced many of the same challenges with regard to security. Each of the companies told Forrester that they needed a different way to manage security because:

- Enterprise applications are increasingly using web-based interfaces so that, to the network, highly-sensitive application data looks identical to data about customers browsing websites.
- External websites are more closely linked to customer data as companies try to enhance the user experience of websites as tools that extend customer relationships beyond the initial purchase.
- Malware and DDoS attacks are able to disrupt the user experience on websites as well as threaten operations by hacking into company desktops or servers.

Situation

Business executives at the CPMC understood the reality and complexity of security attacks; the consensus view of executives recently flipped from accepting that security breaches occur to demanding that security teams anticipate and prepare response strategies. To effectively respond, security teams needed to:

- **Get visibility into end-to-end network traffic.** Security teams needed the ability to monitor the source of intrusion attacks, the applications or data that attackers are targeting, and patterns of routine web traffic and application usage.
- **Secure users from inception through termination.** Security teams needed the ability to provide a secure experience for all users, regardless of the users' location, the type of device, or the applications being accessed.
- **Reduce the time required to manage security policies.** Security teams needed the ability to manage network and application access from a set of central tools rather than managing every application or server individually.
- **Prepare response strategies for security intrusions.** Security teams needed the ability to separate malicious web traffic from legitimate users to manage intrusions or DDoS attacks.

Solution

The CPMC installed three products from F5 Networks — two BIG-IP Local Traffic Managers and one BIG-IP Edge Gateway. The security executives that Forrester interviewed said that using the BIG-IP products gave their security professionals the ability to:

- Isolate the sources of malicious or DDoS attacks and separate attacks from legitimate traffic.
- Identify the internal applications or databases that are being targeted by attackers.
- Leverage companywide databases for user identity and manage users on the network as well as application access privileges from central access management tools.
- Patch known vulnerabilities virtually using iRules almost immediately rather than waiting weeks or months before software vendors release secure product updates.

Results

Forrester's interviews uncovered that by using BIG-IP products, the CPMC is able to:

- **Eliminate standalone firewalls.** The CPMC eliminated 53 standalone firewalls over three years, reducing the cost of annual maintenance fees that the CPMC paid on firewalls, eliminating $190,800 in costs over three years.
- **Secure the user experience on any device.** The CPMC launched its BYOD program with confidence that an end-to-end architecture would protect customer data and other intellectual property.
- **Maintain website availability during DDoS attacks.** On critical shopping days, when the CPMC's online business drives large amounts of revenue, the security team is able to manage DDoS or other malicious attacks without compromising the experience of legitimate customers.
- **Patch vulnerabilities immediately.** Using the iRules platform, the CPMC is able to immediately patch new vulnerabilities until permanent updates are released from software vendors.

Framework Assumptions

Throughout this report, the discount rate used in the present value (PV) and net present value (NPV) calculations is 10%, and time horizon used for the financial modeling is three years. Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult with their respective company's finance department to determine the most appropriate discount rate to use within their own organizations.

Costs

The costs of implementing and using BIG-IP products include licensing products from F5 Networks and training the CPMC's security professionals.

Licensing And Maintaining BIG-IP Solutions

Based on the size and complexity of its operations, the CPMC spends $215,600 over three years in licensing and maintenance fees for two BIG-IP Local Traffic Managers and one BIG-IP Edge Gateway (see Table 2).

Table 2
Licensing And Maintaining F5 BIG-IP Solutions

Ref.	Costs	Calculation	Initial	Year 1	Year 2	Year 3	Total
A1	Application Delivery Controllers	2 units	$110,000				
A2	Edge Gateway	1 unit	$30,000				
A3	Maintenance fees	(A1+A2)*18%		$25,200	$25,200	$25,200	
At	Total costs of licenses		$140,000	$25,200	$25,200	$25,200	$215,600

Source: Forrester Research, Inc.

Training For Security Professionals

To calculate the cost, Forrester includes a five-day on-site course that the CPMC provided as an orientation for the security team. During the first year, the eight security professionals each attended three separate training courses that lasted two days for specific products at a cost of $1,500 per day, resulting in a total cost of $72,000 during Year 1. Over three years, the CPMC's investment in training is $127,000 (see Table 3).

Table 3
Training Security Professionals

Ref.	Costs	Calculation	Initial	Year 1	Year 2	Year 3	Total
B1	Five days of on-site training		$55,000				
B2	Cost of two-day product-specific training course	8*3*2*$1,500		$72,000			
Bt	Total costs		$55,000	$72,000	$0	$0	$127,000

Source: Forrester Research, Inc.

Total Costs

The total cost for the CPMC associated with licensing and maintaining the security solutions from F5 Networks as well as training the security team's use of the products is $342,600 over three years, as shown in Table 4.

Table 4
Total Costs

Ref.	Costs	Calculation	Initial	Year 1	Year 2	Year 3	Total
At	Purchasing solutions		$140,000	$25,200	$25,200	$25,200	
Bt	Training security professionals		$55,000	$72,000			
	Total costs	At+Bt	$195,000	$97,200	$25,200	$25,200	$342,600

Source: Forrester Research, Inc.

Benefits

Based on the interviews, the CPMC gets benefits from using F5 Networks by:

- Eliminating standalone firewalls.
- Securing the migration to BYOD.
- Avoiding outages during DDOS attacks.
- Reducing costs by proactively patching vulnerabilities, including costs for:
  - Server remediation: the cost of downtime to rebuild a server to its original state.
  - Customer triage: the cost of communicating with customers and providing credit protection services.

Eliminating Standalone Firewalls

F5 Networks provides a secure wrapper for users and their application experience, allowing the CPMC to eliminate some of its standalone application firewalls. The CPMC conducted extensive testing of the security provided by F5 Networks before retiring a total of 53 select firewalls.

The price for firewalls used by the CPMC is an average of $20,000 plus an additional maintenance fee of 18% per year — or $3,600 per firewall per year. The financial benefit of retiring 53 firewalls over three years is a cost that the CPMC avoids, totaling $190,800 (see Table 5).

Table 5
Eliminating Standalone Firewalls

Ref.	Benefit	Calculation	Year 1	Year 2	Year 3	Total
C1	Maintenance cost for standalone firewalls	$20,000*18%	3,600	3,600	3,600	
C2	Firewalls eliminated		3	12	38	
Ct	Gross profit benefit	C1*C2	$10,800	$43,200	$136,800	$190,800

Source: Forrester Research, Inc.

Securing Users' BYOD Experience

One of the companies that Forrester interviewed was able to measure the impact of BYOD and reported an increase in net profit of 9% over three years. The benefits came from increased productivity of employees and improved interactions with business partners — largely by managing the overall supply chain of products better. F5 Networks is a key enabler for BYOD because its technology puts a wrapper around the application, the network, and users, eliminating the gaps between security products that could otherwise be exploited in a BYOD environment.

Forrester's model applies the 8.9% benefit to the CPMC as an uplift of 6% in net profit during Year 2 and an additional 3% increase in Year 3. The success of a BYOD initiative depends on many factors, such as web interfaces for applications and integration between mobile and proprietary authentication tools. To measure the impact of F5 Networks on BYOD, Forrester limits the value of security to 5% of the increase in net profit that the CPMC gets through BYOD, resulting in an increase in profit of $614,100 over three years.

Table 6

Securing Users' BYOD Experience

Ref.	Benefit	Calculation	Year 1	Year 2	Year 3	Total
D1	Company net profit	$2 billion*7%	$140,000,000	$140,000,000	$140,000,000	
D2	Business productivity boost		0.0%	6%	3%	
D3	Net profit impact of BYOD	D1*D2		$8,400,000	$4,200,000	$12,600,000
D4	Percent of boost attributable to security		5%	5%	5%	
Dt	Net profit benefit	D3*D4		$420,000	$210,000	$630,000

Source: Forrester Research, Inc.

Avoiding Outages From DDoS Attacks

The security executive in one interview recounted how his company gets more than 60% of its revenue from online sales. On a critical shopping day — Black Friday — the company was subjected to extensive DDoS attacks. BIG-IP products allowed the company to filter malicious traffic from legitimate customers to the extent that the company experienced no complaints from customers and successfully sold products throughout the day.

As show in Table 7, the CPMC suffers two DDoS attacks each year. The average attack lasts six hours and disrupts normal business during that time. Because the CPMC generates $400 million in online revenue at a profit margin of 6.9%, the loss in net profit from a six-hour outage would be $80,769. The impact of avoiding outages during DDoS attacks is $484,615 over three years.

Table 7
Avoiding Outages From DDoS Attacks

Ref.	Benefit	Calculation	Year 1	Year 2	Year 3	Total
E1	Profit from online sales	$400 million*7%	$28,000,000	$28,000,000	$28,000,000	
E2	Duration of typical outage	6 hours/2,080 hours	0.29%	0.29%	0.29%	
E3	Lost profit per outage	E1*E2	$80,769	$80,769	$80,769	
E4	Number of attacks annually		2	2	2	
Et	Gross profit benefit	E3*E4	$161,538	$161,538	$161,538	$484,615

Source: Forrester Research, Inc.

Reduced Cost Of Server Remediation By Proactively Patching Vulnerabilities

The CPMC must address the vulnerabilities that are discovered and announced by software providers. Unfortunately, the permanent patch for any vulnerability usually follows its discovery by several months. F5 Network's solutions include iRules — a platform that allows IT organizations to create custom code that will prevent specific, known vulnerabilities from being exploited.

> *"Being able to immediately close a new vulnerability is priceless. The executives in my company always like to hear that we already have a solution in place. Without iRules, I couldn't say that."* (Director, network security)

During interviews, security professionals told Forrester that iRules reduces the cost of remediating servers that are affected by malware. Using F5, the CPMC eliminates three breaches per year that would have affected the servers. In this case, each breach affects an average of two servers, forcing the servers to be taken offline and restored, which takes an average of two days to rebuild the servers and costs $14,000 per server per breach, including the business that is lost from having a server down that supports customer purchases. The cost for server remediation that the CPMC avoids over three years is a total of $252,000 (see Table 8).

Table 8
Reduced Cost Of Server Remediation By Proactively Patching Vulnerabilities

Ref.	Benefit	Calculation	Year 1	Year 2	Year 3	Total
F1	Reduced number of breaches to servers		3	3	3	
F2	Affected servers per breach		2	2	2	
F3	Cost per server for remediation		$14,000	$14,000	$14,000	
Ft	Avoided costs to remediate servers after breaches	F1*F2*F3	$84,000	$84,000	$84,000	$252,000

Source: Forrester Research, Inc.

Reduced Cost Of Customer Triage By Proactively Patching Vulnerabilities

In addition to the cost to rebuilt servers, some breaches compromise customer data. The CPMC suffers one breach per year that results in a loss of customer data that is caused by security holes in third-party products (e.g., Zero Day Exploits). After a breach, the CPMC typically spends $300 per customer record that is compromised to communicate the breach to customers and provide follow-up support, including credit protection services.

For the CPCM, the one breach per years results in 1,200 customer records being compromised, resulting in a cost of $360,000 per breach. By using iRules to proactively patch vulnerability, the CPMC avoids more than $1 million in costs over three years (see Table 9).

Table 9

Reduced Cost Of Customer Triage By Proactively Patching Vulnerabilities

Ref.	Benefit	Calculation	Year 1	Year 2	Year 3	Total
G1	Reduced breaches to data		1	1	1	
G2	Names affected per breach		1,200	1,200	1,200	
G3	Cost per customer record		$300	$300	$300	
Gt	Avoided cost of customer triage from breaches	G1*G2*G3	$360,000	360,000	360,000	$1,080,000

Source: Forrester Research, Inc.

Total Benefits

The CPMC realizes benefits by using BIG-IP solutions from F5 Networks during a three-year period that total more than $2.5 million (see Table 10).

Table 10
Total Benefits

Ref.	Benefit	Calculation	Year 1	Year 2	Year 3	Total
Ct	Eliminating standalone firewalls		$10,800	$43,200	$136,800	
Dt	Securing the BYOD experience		$0	$420,000	$210,000	
Et	Avoiding outages from DDoS attacks		$161,538	$161,538	$161,538	
Ft	Reduced cost of server remediation		$84,000	$84,000	$84,000	
Gt	Reduced cost of customer triage		$360,000	360,000	360,000	
	Total benefits	Ct+Dt+Et+Ft+Gt	$616,338	$1,068,738	$952,338	$2,637,415

Source: Forrester Research, Inc.

Flexibility

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for some future additional investment. This provides an organization with the right or the ability to engage in future initiatives but not the obligation to do so. There are multiple scenarios in which a customer might choose to implement F5 Networks solutions and later realize additional uses and business opportunities. Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix B).

Using BIG-IP solutions from F5 Networks created future flexibility for:

- **Facilitating central policy management.** F5 Networks secures the network endpoints instead of each application individually, allowing the IT organization to release new applications, add additional users to specific applications, or retire existing applications without changing the security policies. With the purchase of an identify management system, security policies will be centrally managed and rely on the identity management system to coordinate the rights of individual employees across disparate systems. For example, when an employee's permissions change, the central identity and security policies trickle down to specific applications and

are immediately updated. Similarly, when an employee leaves the company, security privileges are revoked across the company, eliminating loose ends such as access rights for employees no longer with the company.

- **Launching and retiring applications.** Using endpoint security policies has the potential to significantly reduce the support burden on security professionals and application managers. As companies increase the pace of spinning up new applications, implementing cloud-based applications (or services), they can migrate from one cloud provider to another, rewrite legacy applications into web-based services, or simply retire legacy applications. Companies are only able to spin up and retire applications quickly when they are logically located within the wrapper provided by BIG-IP products.

Risk

Forrester defines two types of risk associated with this analysis: implementation risk and impact risk. Implementation risk is the risk that a proposed investment in F5 Networks may deviate from the original or expected requirements, resulting in higher costs than anticipated. Impact risk refers to the risk that the business or technology needs of the organization may not be met by the investment in F5 Networks, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for cost and benefit estimates.

Quantitatively capturing investment and impact risk by directly adjusting the financial estimates results in more meaningful and accurate estimates and a more accurate projection of the ROI. In general, risks affect costs by raising the original estimates, and they affect benefits by reducing the original estimates. The risk-adjusted numbers should be taken as realistic expectations since they represent the expected values considering risk.

The following impact risks that affect benefits are identified as part of the analysis:

- **Eliminating some standalone application firewalls.** The ability to eliminate firewalls depends on the current security architecture, the network architecture, and the price that a company pays for firewalls.
- **Supporting and securing the migration to BYOD.** The value of increased productivity from a BYOD strategy will vary depending on the type of work performed by employees and the sensitivity of the work tasks being performed on mobile devices.
- **Avoiding outages from DDOS attacks.** Companies with well-known brand names or that provide services that are considered controversial may suffer levels of malware or attacks that are much higher.
- **Proactively patching vulnerabilities.** The amount of customer data that resides within the company will directly determine the value to be gained through virtual patching.

Tables 10 and 11 show the values used to adjust for risk and uncertainty in the cost and benefit estimates. The TEI model uses a triangular distribution method to calculate risk-adjusted values. To construct the distribution, it is necessary to first estimate the low, most likely, and high values that could occur within the current environment. The risk-adjusted value is the mean of the distribution of those points.

Table 11
Risk Adjustments

Benefits	Low	Most likely	High	Mean
Eliminating some standalone application firewalls	92%	100%	105%	99%
Supporting and securing the migration to BYOD	50%	100%	110%	87%
Avoiding outages from DDOS attacks	80%	100%	103%	94%
Reduced cost of server remediation by proactively patching vulnerabilities	92%	100%	105%	99%
Reduced cost of customer triage by proactively patching vulnerabilities	92%	100%	105%	99%

Source: Forrester Research, Inc.

Table 12
Risk Adjustments To The Three-Year Totals

Benefit	Original value	Risk adjustment	Risk-adjusted value
Eliminating some standalone application firewalls	$190,800	-1%	$188,892
Supporting and securing the migration to BYOD	$630,000	-13%	$548,100
Avoiding outages from DDOS attacks	$484,615	-6%	$455,538
Reduced cost of server remediation by proactively patching vulnerabilities	$252,000	-1%	$249,480
Reduced cost of customer triage by proactively patching vulnerabilities	$1,080,000	-1%	$1,069,200

Source: Forrester Research, Inc.

Readers are urged to apply their own risk ranges based on their own degree of confidence in the cost and benefit estimates.

Financial Summary

The financial results calculated in the Costs and Benefits sections can be used to determine the ROI, NPV, and payback period for the organization's investment in F5 Networks security solutions. These are shown in Table 13 below.

Table 13
Cash Flow — Non-Risk-Adjusted

Cash flow — original estimates						
	Initial	Year 1	Year 2	Year 3	Total	Present value
Costs	($195,000)	($97,200)	($25,200)	($25,200)	($342,600)	($323,123)
Benefits	$0	$616,338	$1,068,738	$952,338	$2,637,415	$2,159,069
Net benefits	($195,000)	$519,138	$1,043,538	$927,138	$2,294,815	$1,835,945
ROI	568%					
Payback period	4.5 months					

Source: Forrester Research, Inc.

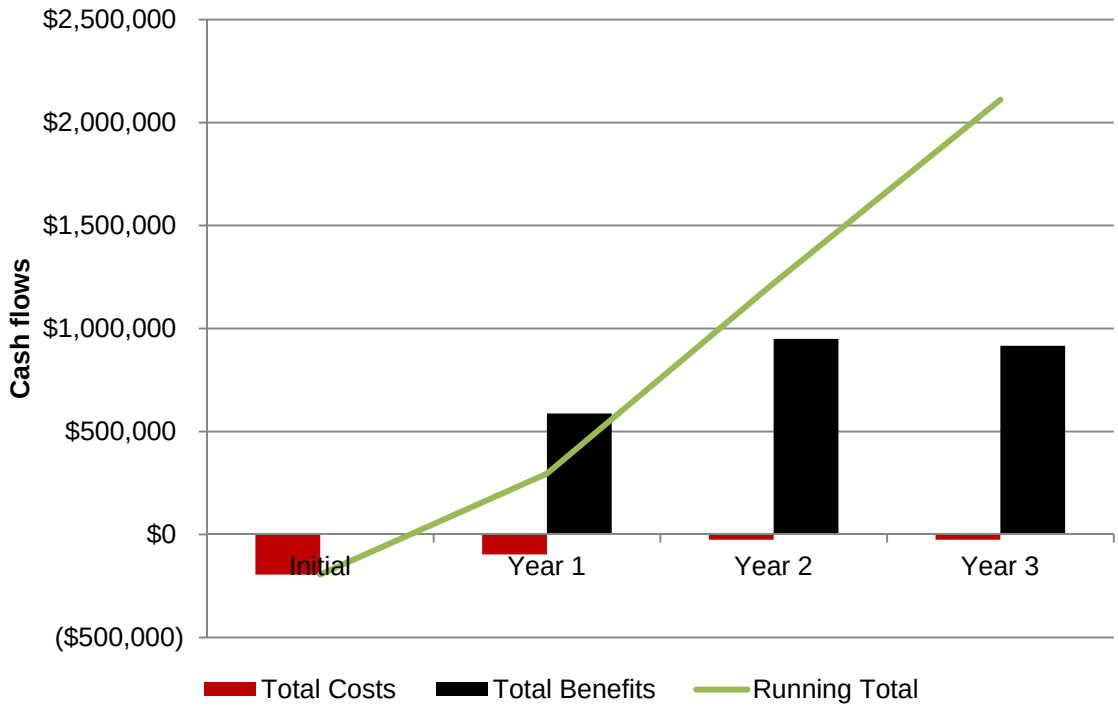
Table 14 and Figure 2 below show the risk-adjusted ROI, NPV, and payback period values. These values are determined by applying the risk-adjustment values from Table 11 in the Risk section to the benefits numbers in Table 10.

Table 14
Cash Flow — Risk-Adjusted

Cash flow — risk-adjusted estimates						
	Initial	Year 1	Year 2	Year 3	Total	Present value
Costs	($195,000)	($97,200)	($25,200)	($25,200)	($342,600)	($323,123)
Benefits	$0	$602,098	$999,574	$909,538	$2,511,210	$2,056,806
Net benefits	($195,000)	$504,898	$974,374	$884,338	$2,168,610	$1,733,683
ROI	537%					
Payback period	4.6 months					

Source: Forrester Research, Inc.

Figure 2
Cash Flows — Risk Adjusted



Source: Forrester Research, Inc.

F5 Networks BIG-IP Security Solutions: Overview

According to F5 Networks, F5 secures access to applications and data from anywhere, while protecting applications wherever they reside. By placing intelligent devices at key points in the network, F5 helps protect resources and minimize interruptions. The BIG-IP family has two categories of solutions: security and access.

- **Security.** The F5 portfolio of products includes BIG-IP Local Traffic Manager (LTM), BIG-IP Advanced Firewall Manager (AFM), BIG-IP Application Security Manager (ASM), and BIG-IP Global Traffic Manager (GTM). These products have the scale, performance, integration of features, and extensibility needed to protect applications in the data center. F5 Security solutions include:
    - **Application delivery firewall (ADF):** A native firewall that provides visibility and control of application security. Customers use ADF to protect networks and application infrastructure in Internet-facing data centers, inspecting as well as offloading SSL and protecting against network-, DNS-, and HTTP/S-based DDoS attacks.
    - **Application security:** Web application firewall that protects against attacks to reduce the risk to intellectual property and data. Customers use ASM to patch security gaps immediately, monitor application vulnerabilities as well as fraudulent activity, and help protect intellectual property.
    - **DDoS:** Defense and mitigation against different layers of DDoS threats, including those that are network-, DNS-, and HTTP/S-based.
- **Identity and access management.** The BIG-IP set of identity and access management solutions simplify authentication, authorization, and accounting (AAA) management. Typical use cases include:
    - Accelerating and securing remote access.
    - Federating identify management.
    - Enhancing web access management.
    - Simplifying virtual desktop management.
    - Streamlining Microsoft Exchange.
- **Mobile security.** F5's mobile security solutions allow employees to work flexibly from any device and any location, while ensuring the security of corporate resources and assets. IT organizations are able to:
    - Protect corporate applications as well as data and simplify device management as well as policy enforcement.
    - Manage individual devices or device groups, push and/or retract applications and data on a device, and lock or wipe only the secure workspace rather than the entire device.
    - Control decisions about content and applications available on each user's devices, including sensitive corporate data that transmits on an app-by-app basis in a secure, encrypted fashion and that is unencrypted only after reaching the enterprise network.

Appendix A: Composite Organization Description

Composite Organization

Based on the interviews with the four existing customers provided by F5 Networks, Forrester has created a composite organization to illustrate the quantifiable costs and benefits of F5 Networks security solutions. The composite company is intended to represent a CPMC and is based on characteristics of the interviewed customers. Specifically, the composite company has:

- **$2 billion in annual revenue.** Although the company sells products globally, this report focuses on business operations, information technology, and security solutions within the US. The CPMC's average profit margin is 6.9%.
- **12,000 employees globally.** Nine thousand employees — or 75% of personnel — are located in the US.
- **Manufacturing facilities in 17 countries.** The company must manage its security policies according to international law, including import and export laws, but this report focuses on complying with regulatory requirements of the US.
- **20% of revenue coming from online sites.** The CPMC has an online site that sells limited products directly to consumers and that provides 20% of annual revenues.
- **Products that are categorized into eight major brands.** Five of the brands have websites that allow consumers to register for information, receive product support, or learn new ways of using the CPMC products.

Appendix B: Total Economic Impact™ Overview

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. The TEI methodology consists of four components to evaluate investment value: benefits, costs, risks, and flexibility.

Benefits

Benefits represent the value delivered to the user organization — IT and/or business units — by the proposed product or project. Often product or project justification exercises focus just on IT cost and cost reduction, leaving little room to analyze the effect of the technology on the entire organization. The TEI methodology and the resulting financial model place 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. Calculation of benefit estimates involves a clear dialogue with the user organization to understand the specific value that is created. In addition, Forrester also requires that there be a clear line of accountability established between the measurement and justification of benefit estimates after the project has been completed. This ensures that benefit estimates tie back directly to the bottom line.

Costs

Costs represent the investment necessary to capture the value, or benefits, of the proposed project. IT or the business units may incur costs in the form of fully burdened labor, subcontractors, or materials. Costs consider all the investments and expenses necessary to deliver the proposed value. In addition, the cost category within TEI captures any incremental costs over the existing environment for ongoing costs associated with the solution. All costs must be tied to the benefits that are created.

Risk

Risk measures the uncertainty of benefit and cost estimates contained within the investment. Uncertainty is measured in two ways: 1) the likelihood that the cost and benefit estimates will meet the original projections, and 2) the likelihood that the estimates will be measured and tracked over time. TEI applies a probability density function known as "triangular distribution" to the values entered. At a minimum, three values are calculated to estimate the underlying range around each cost and benefit.

Flexibility

Within the TEI methodology, direct benefits represent one part of the investment value. While direct benefits can typically be the primary way to justify a project, Forrester believes that organizations should be able to measure the strategic value of an investment. Flexibility represents the value that can be obtained for some future additional investment building on top of the initial investment already made. For instance, an investment in an enterprisewide upgrade of an office productivity suite can potentially increase standardization (to increase efficiency) and reduce licensing costs. However, an embedded collaboration feature may translate to greater worker productivity if activated. The collaboration can only be used with additional investment in training at some future point in time. However, having the ability to capture that benefit has a PV that can be estimated. The flexibility component of TEI captures that value.

Appendix C: Glossary

Discount rate: The interest rate used in cash flow analysis to take into account the time value of money. Although the Federal Reserve Bank sets a discount rate, companies often set a discount rate based on their business and investment environment. Forrester assumes a yearly discount rate of 10% for this analysis. Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult their respective organization to determine the most appropriate discount rate to use in their own environment.

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.

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.

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

Return on investment (ROI): A measure of a project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits minus costs) by costs.

A Note On Cash Flow Tables

The following is a note on the cash flow tables used in this study (see the example table below). The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1. Those costs are not discounted. All other cash flows in Years 1 through 3 are discounted using the discount rate (shown in the Framework Assumptions section) at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations are not calculated until the summary tables and are the sum of the initial investment and the discounted cash flows in each year.

Table [Example]
Example Table

Ref.	Category	Calculation	Initial cost	Year 1	Year 2	Year 3	Total

Source: Forrester Research, Inc.