A Forrester Total Economic Impact™
Study Commissioned By Akamai
August 2019

The Total Economic Impact™ Of Akamai Edge Security Products

Cost Savings And Business Benefits Enabled By Edge Security Products

FORRESTER®

Table Of Contents

Project Director:
Bob Cormier, Vice President
and Principal Consultant

ABOUT FORRESTER CONSULTING

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

FORRESTER®

Benefits

Revenue protection:
$4.7 million

Decommissioning legacy security products:
$125,337

Reduced hardware spend:
$149,211

Security FTE savings:
$1.1 million

Executive Summary

Akamai commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential benefits enterprises may realize by deploying the following Akamai edge security products: Kona Site Defender (KSD), Bot Manager, Prolexic Routed, Enterprise Threat Protector (ETP), and Enterprise Application Access (EAA). The purpose of this study is to provide readers with a framework to evaluate the potential financial benefits these Akamai edge security products have on enterprises.

To better understand the benefits, risks, and flexibility associated with this investment, Forrester directly interviewed several Akamai customers and surveyed 30 more customers with experience using Akamai edge security products.

For this TEI study, Forrester has created a composite *Organization* to illustrate the benefits of investing in Akamai's edge security products. Based on characteristics of the interviewed and surveyed customers, the composite *Organization* is a global, enterprise-sized company with annual revenues of about $1.5 billion.

Prior to using Akamai's edge security products, the *Organization* was using a mix of disparate and costly third-party and homegrown security solutions.

Key Findings

Quantified benefits. The following risk-adjusted present value (PV) benefits total **$5,989,705** over three years and are representative of those experienced by the interviewed and surveyed companies:

- **Cost savings — fewer full-time equivalents (FTE) needed to support Akamai edge security products, $1,052,310.** Compared to its pre-Akamai security environment, the *Organization* saves 2.5 security administrator FTEs in Year 1 (ramp year) and 3.5 FTEs in Years 2 and 3 of our analysis.
- **Revenue protection, $4,662,847.** Prior to its investment in Akamai, the *Organization* was losing revenue due to inadequate security. Akamai helps the *Organization* avoid losing 5% of its revenue and therefore 5% of its resulting gross profit. The $4,662,847 quantified benefit is the gross profit associated with avoiding the loss of revenue.
- **Reduced spending on hardware, $149,211.** The *Organization* would have continued to invest in security infrastructure such as storage, servers, operating system licenses, and annual maintenance to maintain its on-premise legacy security products that were subsequently replaced by Akamai's edge security products.
- **Savings from decommissioning legacy security products, $125,337.** The *Organization* decommissions the following legacy security products: distributed denial-of-service (DDoS), bot management solution, virtual private network (VPN) services, virtual desktop software subscriptions, and single sign-on (SSO) and multifactor authentication (MFA) services.

Unquantified benefits. The interviewed and surveyed customers experienced the following additional benefits, the monetary value of which were not quantified for this study:

FORRESTER®

- Improved site performance during an attack. Estimated load time (in milliseconds) of site during an attack was 101.7 milliseconds before Akamai and 70 milliseconds with Akamai.
- A 5.88% reduction in churn rates and an 11.8% decrease in bounce rates.
- An improvement in click-through rates, a 6.3% improvement in conversion rates, and improved customer satisfaction.

Forrester: The Impact Of A Breach And The Benefits Of Akamai Edge Security Products

- For the 30 customers surveyed, there was an average 65% reduction in number of data breaches and a 27% reduction in the labor cost for remediating a data breach. Each customer reported sleeping better at night knowing Akamai was protecting its internet-facing applications and APIs deployed in their data centers or the public cloud.

Forrester's interviews and surveys with over 35 existing customers and subsequent financial analysis found that the composite *Organization* experienced benefits of $5,989,705 (present value) over three years.

Costs. Interviewed and surveyed customers incurred internal labor costs and Akamai fees associated with their investment in Akamai edge security products. For confidentiality reasons at the request of Akamai, these costs are not quantified in this case study. The cost categories are described in the Costs section. For more information regarding Akamai fees, please contact your Akamai representative.

The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for customers considering an investment in Akamai edge security products.

The objective of the framework is to identify the benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that Akamai edge security products can have on the *Organization*:

DUE DILIGENCE
Interviewed Akamai stakeholders and Forrester analysts to gather data relative to edge security products.

CUSTOMER INTERVIEWS AND SURVEY
Interviewed or surveyed over 35 enterprise customers using Akamai edge security products to obtain data with respect to benefits risks and flexibility.

COMPOSITE ORGANIZATION
Designed a composite *Organization* based on characteristics of the interviewed and surveyed customers.

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

CASE STUDY
Employed three fundamental elements of TEI in modeling Akamai edge security products: benefits, risks and flexibility. Given the increasing sophistication that enterprises have regarding benefit analyses related to IT investments, Forrester's TEI methodology serves to provide a picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

Akamai's Edge Security Products — A Customer Journey

BEFORE AND AFTER AKAMAI'S EDGE SECURITY PRODUCTS

Interviewed And Surveyed Customers

For this study, Forrester conducted five live interviews and surveyed 30 additional Akamai edge security customers. Interviewed and surveyed customers were from North America, EMEA, and APAC and included the following attributes:

- Enterprise-sized, global customers with average annual revenues in the $1.5 billion range.
- Each customer has used at least two of the following Akamai edge security products for more than six months: KSD, Bot Manager, Prolexic Routed, EAA, and ETP.
- 77% of surveyed customers use Akamai's Content Delivery Network (CDN) for website delivery, image delivery, streamed or downloaded video, and API traffic.
- Prior to Akamai, customers were using either third-party solutions or a mix of third-party and homegrown security solutions.

"Using Akamai edge security products has helped us provide consistent service to customers, even during an attack."

83% of surveyed customers

INDUSTRY	REGION	INTERVIEWEE(S)	MONTHS USING AKAMAI PRODUCTS
Technology	APAC	Head of security engineering	12 - 120
Retail	International organization headquartered in the US	Senior cybersecurity manager	48
Financial institution	Europe	• Head of IT infrastructure • Executive vice president	12 - 120
Educational content and technology	International organization headquartered in the US	• Senior director of customer support • Manager, internal systems	18 - 48
Broadcasting	International organization headquartered in APAC	Head of cybersecurity and compliance	12 - 84
30 surveyed customers*	Various	Various	12 - 120

*Data from the 30 surveyed customers was used to support the information and data from the live, in-depth customer interviews.

Key Challenges And Goals

The interviewed and surveyed customers had the following challenges and goals they were hoping to satisfy with an investment in Akamai edge security products:

- To reduce application downtime (and increase application uptime) during malicious attacks.
- To protect intellectual property from data breaches.
- To protect user accounts from credential stuffing and account takeover.

- To simplify and reduce the cost of their IT security environment.
- To protect their brand reputations.

Composite *Organization*

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an associated benefit analysis that illustrates the areas financially affected. The composite *Organization* is representative of the 35 companies that Forrester interviewed or surveyed and is used to present the aggregate financial analysis in the next section. The composite *Organization* that Forrester synthesized from the customer interviews has the following characteristics:

The *Organization* is a global, enterprise-sized company with annual revenues of about $1.5 billion.

- The *Organization* uses the following Akamai edge security products: KSD, Bot Manager, Prolexic Routed, EAA, and ETP.
- It has been using these products for three years.
- An average of 248 applications are protected by Akamai edge security products.
- The *Organization* uses Akamai's CDN for image delivery, streamed or downloaded video, website delivery, and API traffic.

Key Results

Customer interviews and surveys revealed the following quantified benefits from an investment in Akamai's edge security products:

- **Cost savings — fewer FTEs needed to support Akamai edge security products.** Compared to its pre-Akamai security environment, the *Organization* saves 2.5 security administrator FTEs in Year 1 (ramp year) and 3.5 FTEs in Years 2 and 3.
- **Revenue protection.** Akamai helps the *Organization* reduce lost revenue resulting from application downtime, data breach, web fraud, and brand damage by 5%.
- **Reduced spending on hardware.** The *Organization* would have continued to invest in on-premises security infrastructure such as storage, servers, operating system licenses, and annual maintenance to maintain its legacy security products that were subsequently replaced by Akamai's edge security products.
- **Savings from decommissioning legacy security products.** With its investment in Akamai edge security products, the *Organization* decommissions the following legacy security products: DDoS, bot management solution, VPN services, and virtual desktop software subscriptions.

> "If Akamai's capabilities were to be maintained in-house, we would have to hire, train, and retain substantial and expensive security resources. We find that it's more cost-effective to use Akamai's products than attempt to hire and retain scarce security talent."
>
> *Head of security and compliance*

> "Using Akamai edge security products has improved customer satisfaction."
>
> *100% of surveyed customers*

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	Cost savings — fewer FTEs to support edge security	$337,500	$472,500	$472,500	$1,282,500	$1,052,310
Btr	Revenue protection (gross profit) associated with Akamai	$1,875,000	$1,875,000	$1,875,000	$5,625,000	$4,662,847
Ctr	Reduced spending on hardware	$60,000	$60,000	$60,000	$180,000	$149,211
Dtr	Savings from decommissioning legacy security products	$50,400	$50,400	$50,400	$151,200	$125,337
	Total benefits (risk-adjusted)	$2,322,900	$2,457,900	$2,457,900	$7,238,700	$5,989,705

Note: Atr, Btr, Ctr and Dtr refer to risk adjusted totals in the benefit tables below ("r" stands for risk).

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of nearly $5.989 million.

Benefit 1: Cost Savings — Fewer FTEs To Support Edge Security

The *Organization* has invested in the full suite of Akamai's edge security products, including KSD, Bot Manager, Prolexic Routed, ETP, and EAA. Compared to its pre-Akamai security environment, it can now save 2.5 security administrator FTEs in Year 1 (ramp year) and 3.5 FTEs in Years 2 and 3. Interviewed and surveyed customers reported:

- A 26.5% reduction in the hours to recover from an attack with Akamai (309 hours before Akamai; 227 hours with Akamai).
- A 65% reduction in the number of data breaches and a 27% reduction in the labor cost for remediating a data breach.
- A 15% savings in time spent researching and adjusting rule changes with Akamai edge security products.
- Improved ability to protect a broad range of applications from DDoS attacks.
- Reduced workload and time to remediate malware infestations.
- Reduced time required to provision application access or monitor firewall login attempts.
- Labor savings from no longer having to manage multiple appliances. They manage the configuration in one place, then push it out to all Akamai servers. There's also a reduction in risk in terms of getting the policies correct for multiple appliances.
- Labor savings in the reduced volume of attack traffic that Akamai stops, including a reduction in successful attacks to web applications.
- Labor savings from Akamai keeping the *Organization's* web application firewall (WAF) rules up to date.

Risks. Most interviewed and surveyed customers were not yet using the full complement of Akamai edge security products discussed in this case study and therefore reported reduced and variable FTE labor savings.

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

To account for these variations, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $1,052,310.

Cost Savings — Fewer FTEs To Support Edge Security: Calculation Table					
REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Before Akamai — security FTEs required	Interviews	9	9	9
A2	With Akamai — security FTEs required	Interviews	6.5	5.5	5.5
A3	With Akamai — FTEs saved	A1 - A2	2.5	3.5	3.5
A4	Average fully loaded cost — security FTE	Industry average	$150,000	$150,000	$150,000
At	Cost savings — fewer FTEs to support edge security	A3 * A4	$375,000	$525,000	$525,000
	Risk adjustment	↓10%			
Atr	Cost savings — fewer FTEs to support edge security (risk-adjusted)		$337,500	$472,500	$472,500

Benefit 2: Revenue Protection Associated With Akamai

Digital businesses depend on constant, uninterrupted connectivity for the benefit of their customers. Websites, applications, and cloud services are potential targets for DDoS and other attacks, which can significantly harm or even cripple digital businesses.

Interviewed and surveyed customers reported the following benefits of Akamai products, which contribute to preventing revenue loss:

- Reduced application downtime from DDoS attacks
- Reduced costs associated with remediating data breaches (see comment below)
- Reduced web fraud from bots that engage in credential stuffing, fraudulent free trials and coupons, and other malicious activity.
- Protecting their organizations' intellectual property by redirection of bots intending to scrape their websites.
- Reduced lost web traffic by 7.3% and lost views by 10%.
- Reduced lost revenue and resulting gross profit by 5%.

> "I feel very confident in Akamai's ability to protect our valuable data from attacks. Akamai is our front door to all issues and our first line of defense providing protection, and across our cloud computing platform also."
>
> *Head of security and compliance*

Prior to its investment in Akamai, the *Organization* was losing revenue due to inadequate edge security. Akamai helps the *Organization* avoid losing 5% of its revenue and therefore 5% of its resulting gross profit. The $4,662,847 quantified benefit is the gross profit associated with avoiding the loss of revenue. Forrester estimates the gross profit margin to be an overall industry average of 50%.

Risk. The interviewed and surveyed customers had wide ranging total online revenues and different gross margin results.

To account for these variations, Forrester risk-adjusted this benefit downward by 25%, yielding a three-year risk-adjusted total PV of $4,662,847.

Revenue Protection Associated With Akamai: Calculation Table					
REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
B1	Estimated lost revenue	Interviews	$100,000,000	$100,000,000	$100,000,000
B2	Reduction in lost revenue (by 5%)	B1 * 5%	$5,000,000	$5,000,000	$5,000,000
Bt	Revenue protection (gross profit) associated with Akamai	B2 * 50%	$2,500,000	$2,500,000	$2,500,000
	Risk adjustment	↓25%			
Btr	Revenue protection (gross profit) associated with Akamai (risk-adjusted)		$1,875,000	$1,875,000	$1,875,000

Benefit 3: Reduced Spending On Hardware

Interviewed customers shared their experiences with no longer needing on-premises infrastructure platforms for security products, data, computational power, and engineering services. Forrester assumes the *Organization* would have needed to spend $75,000 annually on updating security infrastructure such as storage, servers, operating system licenses, and annual maintenance to maintain its on-premises legacy security products that were subsequently replaced by Akamai's edge security products.

On average, the interviewed customers were saving $75,000 annually on hardware infrastructure for legacy security products.

Risk. The interviewed customers had a wide range of legacy products and costs that required hardware infrastructure. To account for these risks, Forrester risk-adjusted this benefit downward by 20%, yielding a three-year risk-adjusted total PV of $149,211.

"Using Akamai edge security products has helped us reduced churn rates and decrease bounce rates."

83% of surveyed customers

Reduced Spending On Hardware: Calculation Table					
REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
C1	Before Akamai — costs of maintaining on-premises hardware infrastructure	Interviews	$75,000	$75,000	$75,000
Ct	Reduced spending on hardware	C1	$75,000	$75,000	$75,000
	Risk adjustment	↓20%			
Ctr	Reduced spending on hardware (risk-adjusted)		$60,000	$60,000	$60,000

Benefit 4: Savings From Decommissioning Legacy Software Products

Interviewed and surveyed customers reported savings from decommissioning legacy security products that were replaced by Akamai edge security products. The *Organization* was able to decommission the following security products:

- Previous DDoS or bot management solutions.
- VPN services.
- Virtual desktop software subscriptions.

Modeling and Assumptions. On average, the interviewed customers were saving $63,000 annually on various legacy software security products, including some of the products listed above.

Risk. The interviewed and surveyed customers had a wide range of legacy products and costs (some open source) that were replaced by Akamai products. Forrester applied a 20% risk adjustment to reflect these variations in products and cost saved.

Savings From Decommissioning Legacy Security Products: Calculation Table

REF.	METRIC	CALC./SOURCE	YEAR 1	YEAR 2	YEAR 3
D1	Value of decommissioned products	Interviews	$63,000	$63,000	$63,000
Dt	Savings from decommissioning legacy security products	D1	$63,000	$63,000	$63,000
	Risk adjustment	↓20%			
Dtr	Savings from decommissioning legacy security products (risk-adjusted)		$50,400	$50,400	$50,400

Forrester: The Impact Of A Breach And The Benefits Of Akamai Edge Security Products

For the 30 customers surveyed, there was an average 65% reduction in number of data breaches and a 27% reduction in the labor cost for remediating a data breach. Each customer reported sleeping better at night knowing Akamai was protecting its internet-facing applications and APIs deployed in their data centers or the public cloud.

Using Forrester's internal research, we can describe the potential cost categories of a breach.

How much would a breach cost an organization? It depends — on actions taken prior to the breach, the circumstances of the breach itself, and IT's response to the breach. And not all costs are direct, immediately incurred costs. Employee data breaches may affect morale, attrition, and future hiring of skilled talent. Breaches of intellectual property data may directly affect both reputation and the bottom line over several years. There are numerous factors that contribute to costs of a breach; here's a sample list:

- Type of data that was compromised.
- If personal data, number of records and individuals affected.
- Cause of the breach.
- Nature and timing of public disclosure.
- Whether or not the data was encrypted.
- Cyber-insurance.
- A tested incident response plan.
- Customer-facing breach response.

While breach costs can vary widely, there are certain categories of common costs. Readers should consider both direct and indirect costs:

"Using Akamai edge security products has helped us improve click-through rates and conversion rates."

83% of surveyed customers

- **Response and notification.** This includes incident response costs and the operational and service costs for external communications, such as notifying affected individuals or customers as well as the government or regulatory bodies that are required by law.
- **Lost employee productivity and turnover.** Employees are often distracted from their day-to-day duties during a data breach. There may also be downtime as a result of IT taking users or systems offline to curtail the threat.
- **Lawsuits and settlements.** External counsel with expertise in privacy and breach response can guide a response and help meet legal obligations.
- **Regulatory compliance.** Organizations must stay current with the dynamic landscape of regulatory requirements. With the General Data Protection Regulation (GDPR) and upcoming privacy regulations coming in force, organizations will be required to provide all personal data to an individual upon request. This will likely cause operational costs to skyrocket, in addition to the fines organizations would face in the case of a breach.
- **Brand recovery.** Rebuilding trust varies depending on your business and industry. The length of the downturn can also vary depending on the quality of breach response.
- **Additional security and audit requirements.** This includes the cost of fixing infrastructure and onboarding new technology and equipment to remediate the initial cause of breach. It also includes any mandated security and audit requirements resulting from a legal or regulatory settlement.

97% of survey respondents answered yes to: “Are the benefits created by Akamai edge security products greater than the costs, delivering a positive ROI?”

Unquantified Benefits

In addition to the quantified benefits listed above, the interviewed customers also discussed qualitative benefits from using Akamai’s edge security products, including:

- Improved site performance during an attack. Estimated load time (in milliseconds) of site during an attack was 101.7 milliseconds before Akamai and 70 milliseconds with Akamai.
- A 5.88% reduction in churn rates and an 11.8% decrease in bounce rates.
- An improvement in click-through rates, a 6.3% improvement in conversion rates, and improved customer satisfaction.

Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are scenarios in which a customer might choose to implement edge security products and later realize additional business opportunities, including:

- **Flexible cloud choices.** Interviewed customers cited their ability to choose from and across public cloud providers, not having to settle for one cloud provider. They can put Akamai edge security products in front to provide security services in a way that’s agnostic to cloud providers. Having the ability to choose could providers adds flexibility in pricing and services.

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a future additional investment. This provides an organization with the "right" or the ability to engage in future initiatives but not the obligation to do so.

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

Costs

Interviewed and surveyed customers incurred internal labor costs and Akamai fees associated with their investment in Akamai edge security products. For confidentiality reasons at the request of Akamai, these costs are not quantified in this case study. For more information regarding Akamai fees, please contact your Akamai representative. The costs categories are as follows:

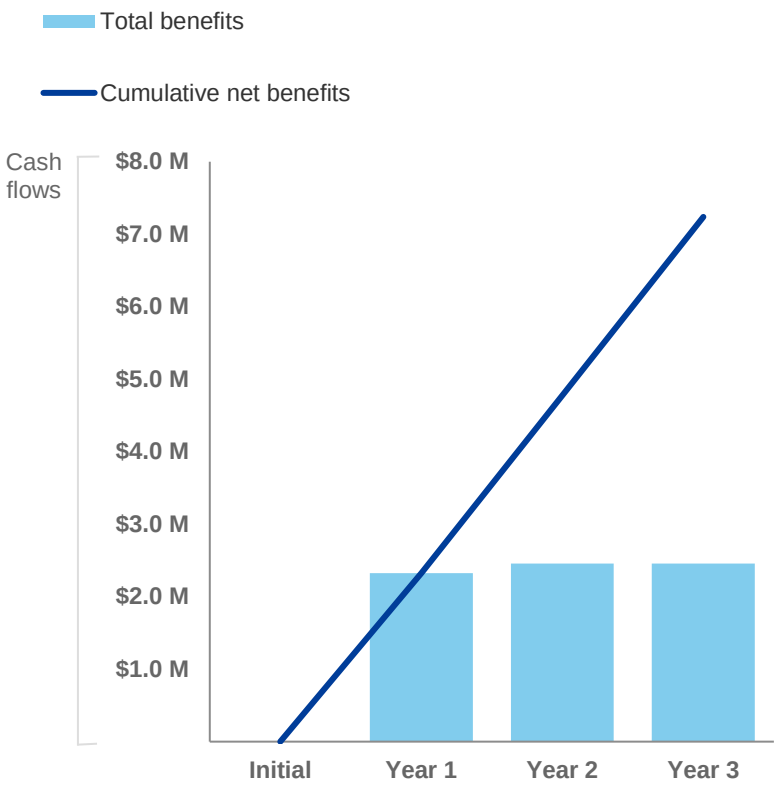
- Internal labor associated with vendor selection, preplanning the implementation, and actual implementation of Akamai's edge security products. This involved 10 FTEs working part-time over four weeks, including the CISO, security engineers, network engineers, and developers.
- Ongoing internal labor associated with managing the Akamai products and maintaining the vendor relationship with Akamai. This involved 1.5 security engineers monitoring the products and researching and adjusting rule changes with Akamai edge security products along with other security-related duties.
- Akamai's fees, which include clean traffic rates, license/subscription fees, professional services, and training.

Compared to its pre-Akamai security environment, the *Organization* saves 3.5 security administrators with Akamai.

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Benefit Chart (Risk-Adjusted)



Forrester assumes an annual discount rate of 10% for this present value benefit analysis.

These risk-adjusted benefit values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit section.

Benefits (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total benefits	$0	$2,322,900	$2,457,900	$2,457,900	$7,238,700	$5,989,705

FORRESTER®

Akamai Edge Security Products: Overview

The following information is provided by Akamai. Forrester has not validated any claims and does not endorse Akamai or its offerings. Below is a brief description of each Akamai Edge security product included in this case study.

Kona Site Defender

- Complete application protection
- Reduces risks of downtime, data theft, and website defacement
- Protects against the largest DoS and DDoS attacks
- Protects against web attacks such as SQL injection, XSS, and RFI

Enterprise Application Access

- Application Access Redefined: Secure, Simple, Fast
- Centralize your security and access control
- Keep all users off your network and make your applications invisible to the internet
- Complete auditing and reporting of user activity

Enterprise Threat Protector

- Proactive protection against zero-day malware
- Proactive protection vs. reactive mitigation
- Instant protection without complexity or hardware
- Quick and uniform enforcement of Acceptable Use Policy

Prolexic solutions

- Expert mitigation against the broadest range of DDoS attacks with industry-leading SLAs
- Reduces business risks posed by the threat of DDoS attack
- Maintains availability of internet-facing applications
- Fast mitigation by Akamai's 24x7 SOC, with time-to-mitigate SLA

Bot Manager

- Advanced strategies to flexibly manage the long-term business and IT impact of bots
- Provides visibility into the amount of bot traffic accessing your site
- Improves user experience by reducing the impact of bots on the web during peak traffic hours
- Prevents price and content scraping

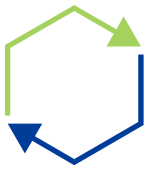
Appendix A: Total Economic Impact

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.