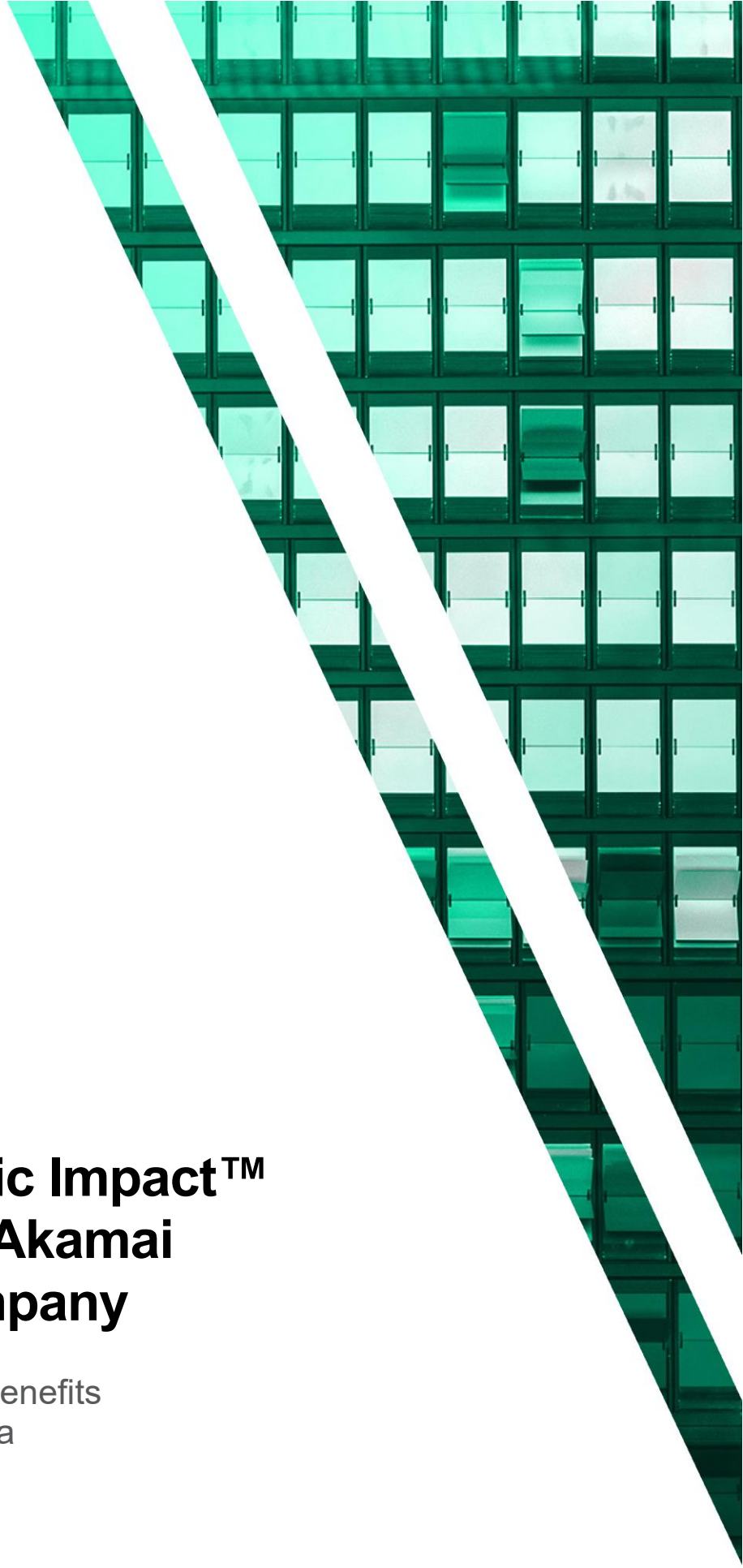
FORRESTER®



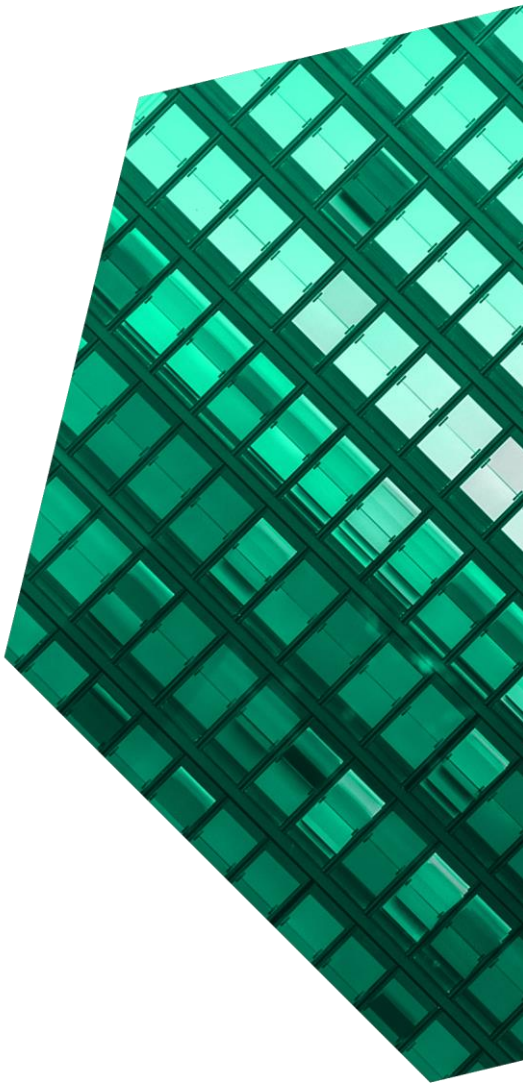
The Total Economic Impact™ Of Guardicore An Akamai Technologies Company

Cost Savings And Business Benefits Enabled By Guardicore Centra

November 2021

Table Of Contents

Consulting Team: Robert Crockett



Executive Summary

Complex IT ecosystems coupled with fragile security protocols leave companies vulnerable to security attacks. As companies move towards Zero Trust, microsegmentation solutions help protect against unknown exposures on the network. Guardicore's Centra Security Platform deploys an infrastructure-agnostic, agent-based approach to increase network visibility and security, enabling enterprise network security platforms to be more dynamic and agile while protecting against malicious actors.

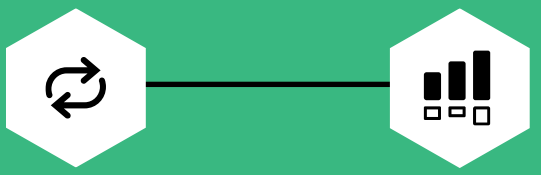
Organizations are continuously responding to changes in the cybersecurity landscape and evaluating their cybersecurity strength and posture. However, a lack of visibility across a network precludes their ability to make simple changes quickly and easily. Guardicore's Centra platform enables organizations to dynamically create, implement, and deploy more granular security policies across applications and endpoints.

Guardicore commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Guardicore Centra.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Guardicore Centra on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five decision-makers with experience using Guardicore Centra. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization.

Prior to using Guardicore Centra, interviewees noted how their organizations suffered from a lack of network visibility, which prevented them from executing strategic security goals. Legacy microsegmentation solutions were not intuitive and did not increase network agility or sophistication.

KEY STATISTICS



Return on investment (ROI)
106%

Net present value (NPV)
$4.12M

Organizations had limited success with expensive homegrown solutions to ring-fence applications and endpoints. Time-consuming efforts to create and deploy effective security policies were ineffective as well. These limitations led to inefficiencies in identifying and patching security breaches, an influx of endpoints losing VPN network connectivity, and an inability to provide a sufficient level of security to satisfy regulatory requirements.

After the investment in Guardicore Centra, the interviewees' organizations streamlined their risk posture and policy management capabilities and drastically enhanced their visibility across applications and endpoints. This enabled them to intuitively visualize east-west traffic on the network. Key results from the investment include increased security operations (SecOps) and IT operations productivity, reduced incident management effort, and reduced probability of a security breach. The solution also reduced the cost of upgrading existing

firewalls and hardware appliances. These results created a stronger security environment and reduced network infiltration exposure size.

Increased security operations productivity

95%

KEY FINDINGS

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

- **Streamlined posture and policy management capabilities, which increased security operations productivity by 95% for the composite organization.** Most interviewees had limited capabilities in developing, building, and deploying posture policy, and most of what they had was manual. These workflows resulted in inefficient and time-consuming operational efforts that hinder development speeds. Manually enforcing policy also introduces risk and limits an organization's ability to scale security controls. Using Guardicore Centra, organizations greatly reduced the effort required to implement and enforce policy.
- **Reduced time spent performing incident management efforts by roughly 65% for the composite organization.** Reducing the effort needed to investigate and remediate the average network alert or incident across security and IT operations teams is becoming increasingly important as clandestine network threats become more difficult to identify and thwart. Over three years, the present value of incident management efforts that are no longer needed with Guardicore Centra is worth nearly $3.3 million to the composite organization.
- **Reduced the cost to maintain existing network hardware appliances by $236,000 per year for the composite organization.** In addition to reducing the size of the hardware appliances within their networks, interviewees noted their organizations eliminating costs associated with extraneous network hardware appliances. Interviewees also noted that the previously used tools provided only some of the

Guardicore takes input better than anybody else. They will take your request for enhancement […] and then they will make their product better. They look at what their customer needs, and they will implement it because it's going to bring you closer to success.

— Director of security, financial services

capabilities that the Guardicore Centra platform offers.

- **Enhanced network visibility for data breach avoidance and reduced infiltration exposure, translating to nearly $589,000 a year for the composite organization.** As malware and ransomware attacks continue to be top of mind for chief technology officers and chief data officers, maintaining the highest level of data and privacy protection is paramount for organizations. Furthermore, failures to prevent major network breaches can be extremely costly. Accounting for the potential cost and lowered probability of a security breach, the composite organization saves nearly $589,000 annually.
- **Avoided investing in upgrades to the composite organization's existing network firewall infrastructure, providing benefits worth nearly $2.0 million.** Interviewees shared examples of failed attempts to effectively implement microsegmentation with homegrown solutions, which in all cases were comprised of a network of firewalls. As regulatory requirements and business objectives shifted, so too did network infrastructure and the accompanying need to upgrade the existing network of firewalls. With Guardicore Centra, the interviewees' organizations were able to reduce the count of firewalls by 70 to 80%.

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

- **Guardicore's commitment to customer success, which enabled organizations to identify additional use cases.** Interviewees repeatedly noted the value their organizations have received from the ongoing support of Guardicore's professional services team. This support encouraged organizations to expand the scope of services to address additional use cases. A director of enterprise security in telecommunications noted, "There were probably a dozen or more use cases that we identified, and [Guardicore] worked together with our team to build and test configurations that solved specific use cases."
- **Consolidated security controls, which encouraged organizations to continue developing their IT infrastructure.** The level of sophistication associated with the platform's dynamic interface created ease of use to automate network security capabilities. This enabled organizations to create more advanced and streamlined IT infrastructure.

Costs. Risk-adjusted PV costs include:

- **Upfront costs, which include deployment, implementation, training, and professional services, and account for $162,000 to the composite organization.** The deployment and implementation for initial and additional use cases (including hardware and software integrations, proof-of-concept, and training), as well as initial professional services fees were all expressed as part of the overall upfront costs associated with the solution. This cost is proportional to the number of licenses that were purchased by the interviewees' organizations.
- **Licensing fees and costs associated with ongoing solution development and maintenance totaling over $3.7 million to the composite organization.** Solution development and maintenance, including hardware and software integrations, ongoing professional services fees, and monitoring and enforcement fees, all contributed to the ongoing costs of the solution.

The decision-maker interviews and financial analysis found that a composite organization experiences benefits of about $8 million over three years versus costs of $3.88 million, adding up to a net present value (NPV) of $4.12 million and an ROI of 106%.

ROI
106%

BENEFITS PV
$8.00M

NPV
$4.12M

PAYBACK
12 months

Benefits (Three-Year)

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 Guardicore Centra.

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 Guardicore Centra can have on an organization.

DUE DILIGENCE

Interviewed Guardicore stakeholders and Forrester analysts to gather data relative to Guardicore Centra.

DECISION-MAKER INTERVIEWS

Interviewed five decision-makers at organizations using Guardicore Centra to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees' organizations.

FINANCIAL MODEL FRAMEWORK

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

CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Guardicore Centra Customer Journey

Drivers leading to the Guardicore Centra investment

Interviewed Decision-Makers

Interviewee	Industry	Region	Number of Employees
Director of security	Financial services	Switzerland	72,000
Director of enterprise security	Telecommunications	US	5,100
Senior manager, security and innovation	Telecommunications	Brazil	12,000
IT architect	Information technology	Denmark	4,000
Network infrastructure architect	Food retail	US	1,000

KEY CHALLENGES

A typical before state of Guardicore Centra customers included a network of internal and external firewalls, as well as external software visibility tools. Posture and policy management were largely manual, and efforts to segment using homegrown solutions or other vendors lacked the controls and features so organizations could easily monitor and manage network security.

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

- **Inefficient investigation and remediation protocols from a failure to improve central security.** Interviewees' organizations sought a new way to analyze and understand application and endpoint communication across a global IT environment to effect positive change from a security standpoint. Additionally, the desire for near-immediate threat relief was not met with previous solutions.
- **Limited visibility across endpoints prevented organizations from proactively reducing network attack surface area.** Controlling network traffic or isolating systems and applications was almost entirely reactive and automating policy deployment was challenging. Prior solutions lacked the intuitiveness and vision to allow organizations to be as flexible as possible.
- **Complex network architecture made deploying microsegmentation, as well as deploying and enforcing policy, time-consuming and resource-intensive.** Efforts to understand internal networks and microsegmentation tools with homegrown solutions or a network of firewalls were arduous and relatively expensive compared to external solutions. Additionally, some external solutions lacked ease of use or could not meet the organizations' expectations.

> **"We wanted visibility. We wanted to be able to control [our network] at a moment's notice. We wanted to be able to put very specific and granular rules into place that stop certain traffic, but allow it during certain times of the day or under extreme circumstances. We wanted something that was extremely robust and gave us a lot of capabilities."**
> *– Director of enterprise security, telecommunications*

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Improve overall security posture using granular policy to ring-fence applications and reduce the attack surface across the network.
- Eliminate the need to build homegrown middleware solutions as a form of network security enhancement.
- Reduce network complexity while enhancing visibility to ensure cross-environment connections are secure and geographic traffic across hosts is not being shared.
- Streamline microsegmentation and policy creation by offering a single, centralized workflow to define assets and simplify application dependency mapping.
- Enhance user ability to dive deep into specific network segments and identify root cause issues as well as set new policy and enforce new rules on like-environments across a network.

COMPOSITE ORGANIZATION

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

Description of composite. The global financial services organization provides commercial banking, investment banking, asset management, wealth management, and investor services as well as high-volume customer support for its financial products. The composite organization has a strong brand, global operations, a large customer base of about 10 million clients, and a strong presence in the financial services industry. While the composite organization is a large enterprise, the Guardicore solution supports organizations both small and large across a diverse list of industries.

Deployment characteristics. The composite organization has global operations across 10 countries and its network is comprised of 7,500 physical and virtual servers. Additionally, the business routinely makes hardware updates to the existing IT infrastructure every three to five years to remain at the forefront of industry best practices and to stay ahead of the curve in terms of network security regulatory compliance.

Key assumptions

- **$2.5 billion in revenue**
- **5,000 employees**
- **18,000 agents**
- **7,500 servers**

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	Increased security operations productivity	$362,794	$362,794	$362,794	$1,088,381	$902,214
Btr	Reduced incident management effort	$1,323,878	$1,323,878	$1,323,878	$3,971,635	$3,292,290
Ctr	Reduced cost to maintain existing network hardware appliances	$0	$236,250	$236,250	$472,500	$372,746
Dtr	Cost avoidance of a security breach	$589,050	$589,050	$589,050	$1,767,150	$1,464,880
Etr	Cost avoidance of upgrading legacy firewalls	$0	$1,246,875	$1,246,875	$2,493,750	$1,967,271
	Total benefits (risk-adjusted)	$2,275,722	$3,758,847	$3,758,847	$9,793,416	$7,999,401

INCREASED SECURITY OPERATIONS PRODUCTIVITY

Evidence and data. Efficiency gains in the decision-makers' organizations' security operations were typically realized based on the degree of policy deployment and enforcement in prior environments. With Guardicore Centra, SecOps teams could now easily view microsegmentation and policy creation in a single workflow, as well as simplify posture validation.

- Prior microsegmentation and network visibility solutions lacked control. This resulted in organizations performing manual intervention to investigate, isolate, and understand illegitimate east-west traffic throughout a complex network.
- Organizations lacked a clear understanding of their IT environments, which limited their insights into how applications and end users communicated with databases throughout the network.
- Management of network hardware in terms of defining and deploying policy was reduced by 95%.
- When asked what the impact of increased visibility across the network has been using prior network visibility solutions, a director of enterprise security for a telecommunications company said, "We don't have that capability with other products today."

Modeling and assumptions. In the case of the composite organization, Forrester assumes that there is a dedicated team responsible for incident management efforts.

- The composite company employs a team of eight security operations workers. This team focuses exclusively on designing, building, deploying, and enforcing policy.
- The effort to design, build, deploy, and enforce policy across a multi-cloud and hybrid environment previously takes nine months, but with Guardicore Centra this shrinks to two weeks.

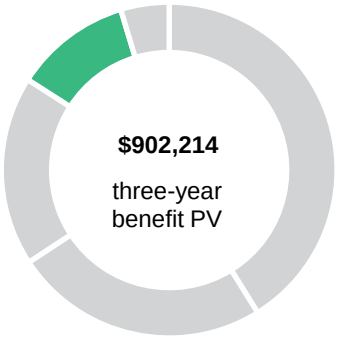
"With the tools Guardicore has, it's easy to see traffic, it's easy to create rules, and it's easy to safely filter out the rules that shouldn't be there. I updated all of our applications and had zero end user downtime."
– Network infrastructure architect, food retailer

- From the increase in productivity, the security operations workers recapture 50% of the time that would have been spent on posture and policy management. This time is redirected towards other projects and business needs.

Risks. The impact of this benefit can be lower for organizations given:

- The efficiency with which organizations carry out policy deployment and enforcement.
- The speed with which an organization applies rules and policies across a network in their prior environment.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of over $902,000. This is equivalent to additional productivity worth almost $113,000 (in PV) per security operations worker achieved over the course of three years.



Increased Security Operations Productivity

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Number of security operations workers	Composite	8	8	8
A2	Hourly rate per security operations worker	Assumption	$72	$72	$72
A3	Number of hours performing SOC management (prior state)	Assumption	1,560	1,560	1,560
A4	Reduced time to create and enforce policy	Interviews	95%	95%	95%
A5	Number of hours saved performing SOC management (after Guardicore Centra)	A3*A4	1,482	1,482	1,482
A6	Percent captured	Composite	50%	50%	50%
At	Increased security operations productivity	A1*A2*A5*A6	$426,816	$426,816	$426,816
	Risk adjustment	↓15%			
Atr	Increased security operations productivity (risk-adjusted)		$362,794	$362,794	$362,794
	Three-year total: $1,088,381			**Three-year present value: $902,214**	

REDUCED INCIDENT MANAGEMENT EFFORT

Evidence and data. The interviewed decision-makers repeatedly mentioned the reduction of time and effort spent around incident management as a benefit of Guardicore Centra. Many went on to state that their organizations had a vulnerable network surface area that security operations teams did not even know existed prior to investing in the product. An IT architect for an information technology firm noted the new ability to recognize and act upon these vulnerabilities, stating, “Light was shed across vulnerabilities that we didn’t even realize we had, let alone had to protect.”

- Threat detection across applications and databases was very time-consuming due to the complex network architecture. This issue coupled with a lack of central security controls made efforts to investigate and remediate threats inefficient.
- Organizations were unable to deliver more granular segmentation capabilities, which prevented them from improving network security strategy. In one case, a security audit revealed that system controls did not comply with regulatory requirements, spurring the need to invest in and develop network security as quickly as possible.

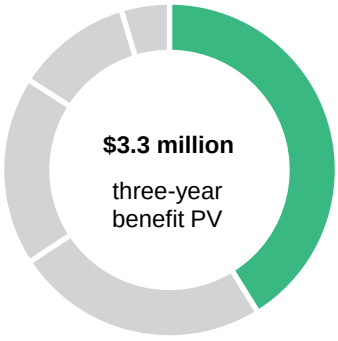
Modeling and assumptions. For the composite organization Forrester assumes:

- The composite organization has a dedicated team responsible for investigating and remediating security alerts. This team is comprised of eight security operations workers and eight IT operations workers.
- This dedicated team spends the entirety of their daily efforts investigating and patching security threats. Given that not all freed-up time necessarily goes back into productive use of identifying and remediating network alerts, a 65% productivity conversion rate has been applied given the robust capabilities of the solution.

Risks. The impact of this benefit can be lower for organizations given:

- The complexity of an organization’s IT infrastructure, especially relating to security operations and IT operations teams’ abilities to investigate and remediate security threats.
- The size of given security operations and IT operations teams that are dedicated to incident management.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of almost $3,300,000.



Reduced Incident Management Effort					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Number of security operations and IT operations workers	Composite	16	16	16
B2	Hourly rate per worker	Assumption	$68	$68	$68
B3	Number of hours worked performing threat detection and remediation	Assumption	2,080	2,080	2,080
B4	Reduced incident management effort	Composite	65%	65%	65%
B5	Hours saved performing incident management efforts	B3*B4	1,352	1,352	1,352
Bt	Reduced incident management effort	B1*B2*B5	$1,470,976	$1,470,976	$1,470,976
	Risk adjustment	↓10%			
Btr	Reduced incident management effort (risk-adjusted)		$1,323,878	$1,323,878	$1,323,878
	Three-year total: $3,971,635			**Three-year present value: $3,292,290**	

REDUCED COST TO MAINTAIN EXISTING NETWORK HARDWARE APPLIANCES

Evidence and data. Interviewees' organizations' solutions before Guardicore Centra were not agile in terms of controlling traffic or easily isolating an application or database and did not offer similar levels of network visibility. A director of enterprise security for a company in the telecommunications industry noted that their organization's prior solution was more challenging to use and required an arduous process to gain functional control.

Reduced count of network firewalls

75%

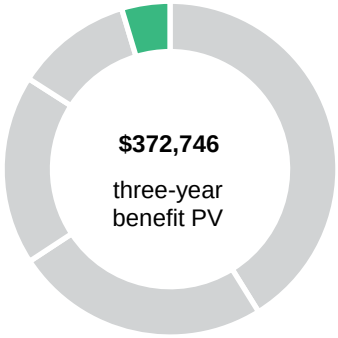
Modeling and assumptions. For the composite organization Forrester assumes:

- External network hardware appliance maintenance and support costs would be roughly 20% of the cost of upgrading legacy firewalls.
- No hardware appliances were reduced in Year 1 to ensure that resources were not taken away from the prior solution until the composite organization saw the effectiveness of the new platform.

Risks. The impact of this benefit can be lower for organizations given:

- The level of integration that networks had with external appliances and the number of network visibility tools that were leveraged in the prior environment.
- The age and overall level of maintenance required by network appliances in the prior environment.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of almost $373,000.



Reduced Cost To Maintain Existing Network Hardware Appliances

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Cost of existing network appliances	Et	$0	$1,312,500	$1,312,500
C2	Maintenance and support of existing network appliances	Composite	20%	20%	20%
Ct	Reduced cost to maintain existing network hardware appliances	Sum of C2 (to date)	$0	$262,500	$262,500
	Risk adjustment	↓10%			
Ctr	Reduced cost to maintain existing network hardware appliances (risk-adjusted)		$0	$236,250	$236,250
	Three-year total: $472,500		**Three-year present value: $372,746**		

COST AVOIDANCE OF A SECURITY BREACH

Evidence and data. Organizations are always conscious of improving their network security capabilities; many firms devote considerable efforts to meeting regulatory requirements and industry best practices. Overall security posture is improved continuously, as is the effort to reduce the potential attack surface. This required application ringfencing through granular policy.

- Interviewees conveyed to Forrester that without Guardicore's monitoring and enforcement capabilities, malicious actors on their organizations may not have been identified due to the lack of visibility that endpoints had with applications across the network.
- According to the Ponemon Institute, the average number of days to identify and contain a data breach is 287-324 days.[2]

Interviewed decision-makers cited that the effort to identify and remediate potential security threats was reduced dramatically thanks to improved visibility, an enhanced security environment, and a reduction in infiltration exposure.

Modeling and assumptions. For the composite organization Forrester assumes:

- The composite organization has some of its environment in the cloud, making security across a hybrid cloud infrastructure important. Many cloud services provide some security, but it is often not enough to protect critical assets or eliminate human error or manual misconfiguration of security systems. Due to these complexities, Forrester estimates the likelihood that a security breach would not be caught by existing security policy management is 15%.

Reduced potential cost of a security breach

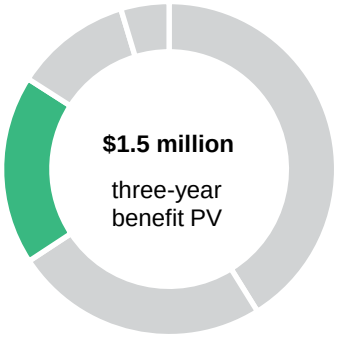
$4.6 million

- The composite organization would likely incur a remediation cost of $4.62 million per exposure based on the average cost of a data breach in the financial services industry as reported by the Ponemon Institute in 2021 and its size.[3]

Risks. The impact of this benefit can be lower for organizations given:

- The level of security and endpoint encryption software vendors that were connected to the system prior to the implementation of Guardicore Centra.
- The type of attack and frequency with which malicious actors target businesses like the composite organization.
- The number of security threats to which organizations can expect to be exposed yearly.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of almost $1,465,000.



Cost Avoidance Of A Security Breach

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Potential exposure	Ponemon	$4,620,000	$4,620,000	$4,620,000
D2	Probability of exposure (incremental savings credited to Guardicore Centra, based on level of complexity of environment)	Forrester research	15%	15%	15%
Dt	Cost avoidance of a security breach	D1*D2	$693,000	$693,000	$693,000
	Risk adjustment	↓15%			
Dtr	Cost avoidance of a security breach (risk-adjusted)		$589,050	$589,050	$589,050
	Three-year total: $1,767,150			**Three-year present value: $1,464,880**	

COST AVOIDANCE OF UPGRADING LEGACY FIREWALLS

Evidence and data. Interviewees noted one of the primary reasons for their organizations exploring Guardicore Centra was to find alternatives to the prior solution, as well as evaluating and making upgrades to current microsegmentation capabilities. In customers' prior environments, several also noted the extensive use of firewalls for segmenting applications, many of which were due to be upgraded within a few years to comply with regulatory requirements or industry best practices.

- Interviewed decision-makers' organizations had internal and external networks of firewalls that were used for standard network security monitoring and were also used as homegrown solutions to segment internal zones across different business functions within the networks.
- A network infrastructure architect at a food retailer noted that a vendor recommended Guardicore Centra as a potential solution to the organization's need to upgrade their existing firewall network. This recommendation spurred the organization to seek a demonstration from Guardicore, followed by a request for Guardicore to build a proof of concept. From this information, Forrester recognized that avoiding upgrading legacy firewalls was their primary use case.
- The associated cost of individual firewalls is an average of the per-unit costs amongst the total number of firewalls.

Modeling and assumptions. For the composite organization Forrester assumes:

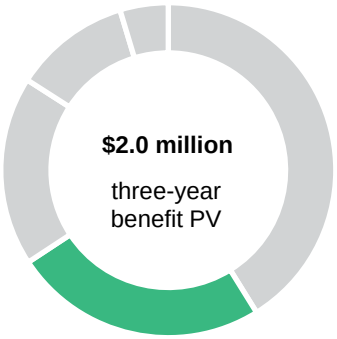
- The average cost of the 75 enterprise-grade firewalls the composite organization uses is $35,000 each.[4]
- The composite organization considers alternative homegrown segmentation solutions prior to realizing that the entire network of firewalls would need to be upgraded.
- The complete network of firewalls would be upgraded in Year 2 and Year 3 as necessary with 50% of the firewalls to be upgraded each year.

> **"We've never been able to do network segmentation in such a way that we could keep track of it and make sure it was set up correctly. It was something we wanted to do for many years and couldn't do until we got Guardicore."**
> *– IT architect, information technology*

Risks. The impact of this benefit can be lower for organizations given:

- Number and relative cost of existing networks or internal and external firewalls, as well as the level of regulatory network security compliance towards which a given organization is working.
- The aggressiveness with which organizations choose to undertake any upgrades to the network of firewalls, and the associated time in which those upgrades are completed.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of almost $1,970,000.



Cost Avoidance Of Upgrading Legacy Firewalls					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
E1	Number of legacy firewalls	Composite	75	75	75
E2	Cost per firewall	Assumption	$35,000	$35,000	$35,000
E3	Percent captured	Assumption	0%	50%	50%
Et	Cost avoidance of upgrading legacy firewalls	E1*E2*E3	$0	$1,312,500	$1,312,500
	Risk adjustment	↓5%			
Etr	Cost avoidance of upgrading legacy firewalls (risk-adjusted)		$0	$1,246,875	$1,246,875
	Three-year total: $2,493,750			**Three-year present value: $1,967,271**	

UNQUANTIFIED BENEFITS

Additional benefits that customers experienced but were unable to quantify include the following:

- **Guardicore's commitment to customer success, which enabled organizations to identify additional use cases.** Interviewees noted that Guardicore's professional services team helped their organizations realize additional benefits and use cases. They said that Guardicore had exceptional capabilities in terms of helping customers to create policy as well as performing any automation or customized tasks. A director of security in the financial services industry remarked, "If there is a business feature that makes sense and is valuable to your organization, Guardicore will build a solution around your specific use case."
- **Consolidated security controls encouraged organizations to streamline their IT infrastructure.** Interviewed decision-makers reported that the Guardicore Centra platform had an intuitive user interface that centralized all security controls in a manner that makes microsegmentation and threat detection much simpler for end users.

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Guardicore Centra and later realize additional use cases and opportunities, including:

- **Securing cloud-based containerized workflows across a multi-cloud program.** In the context of managing and securing applications across a multi-cloud program, Guardicore Centra enabled customers to secure both production and operational elements of their containers by visually highlighting the communication of containers and virtual machines (VMs).
- **Segmenting across a larger portion of VMs within internal networks using compiled labeling data.** Once organizations recognized the robust nature of the AI-enabled labeling capabilities of Guardicore Centra, organizations cited growth in the scope of application segmentation. The amount of labeling data that was compiled enabled businesses to deliver on network development initiatives more quickly.

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**
Ftr	Upfront costs (deployment, implementation, training, professional services, etc.)	$135,700	$28,750	$0	$0	$164,450	$161,836
Gtr	Ongoing costs (licensing fees, ongoing solution development and maintenance, etc.)	$1,019,700	$1,056,011	$1,087,520	$1,119,974	$4,283,204	$3,719,939
	Total costs (risk-adjusted)	$1,155,400	$1,084,761	$1,087,520	$1,119,974	$4,447,654	$3,881,775

UPFRONT COSTS (DEPLOYMENT, IMPLEMENTATION, TRAINING, PROFESSIONAL SERVICES, ETC.)

Evidence and data. There are upfront costs to the Guardicore Centra solution, which varied based on the level of administration that was sought by the interviewees.

- In general, the decision-makers organizations were impressed with the level of sophistication Guardicore presented to them during the proof-of-concept phase, which encouraged them to deploy the solution in a relatively short period of time after monitoring the test environment.
- Interviewees applauded the level of customization that Guardicore provided to their organizations, which encouraged them to purchase additional ongoing professional services and deploy the solution across additional use cases.

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

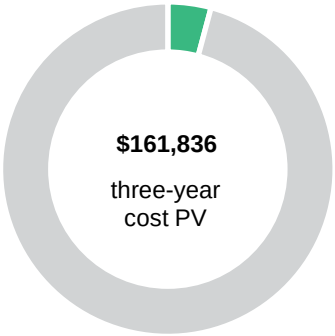
- The two network architects and two network administrators used in the model are based on the 18,000 agents employed by the composite organization. They will work at a rate of $50 per hour during the six weeks of deployment.
- The upfront charges in the initial year covering training, complimentary professional services, and deployment will amount to $70,000.
- Additional use cases for the platform were not covered in the initial proof-of-concept build and testing phases prior to deployment. Instead, the composite organization was impressed with the large amount of labelling data that the solution provided, which encouraged the organization to have Guardicore Centra build and test another use case the following year.
- Deployment, implementation, and additional use-case costs are representative of an aggregated cost of services and are based on assumptions made about the composite organization.

Risks. The impact of this cost may be higher for organizations given:

- The number of use cases that are contractually agreed upon prior to implementation, as well as the number of agents across which the solution is deployed.

- The complexities of prior IT infrastructure that affect time to develop and test a proof-of-concept.
- The level of dependence that the organization places on Guardicore to develop custom tools and capabilities from the solution.

Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of almost $162,000.



Upfront Costs (Deployment, Implementation, Training, Professional Services, Etc.)

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Number of internal network architects and administrators	Composite	4	0	0	0
F2	Hourly rate per worker	Composite	$50	$0	$0	$0
F3	Hours	Assumption	240	0	0	0
F4	Deployment costs	F1*F2*F3	$48,000	$0	$0	$0
F5	Implementation costs (inclusive of training, professional services, and deployment costs)	Assumption	$70,000	$0	$0	$0
F6	Additional use case	Assumption	$0	$25,000	$0	$0
Ft	Upfront costs (deployment, implementation, training, professional services, etc.)	F4+F5+F6	$118,000	$25,000	$0	$0
	Risk adjustment	↑15%				
Ftr	Upfront costs (deployment, implementation, training, professional services, etc.) (risk-adjusted)		$135,700	$28,750	$0	$0
	Three-year total: $164,450			**Three-year present value: $161,836**		

ONGOING COSTS (LICENSING FEES, ONGOING SOLUTION DEVELOPMENT AND MAINTENANCE, ETC.)

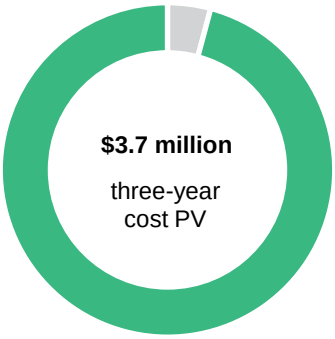
Evidence and data. The licensing costs of Guardicore Centra at the organizational level are based on the number of agents within the network that are covered by the solution, as well as the number of use cases that were contractually agreed upon prior to deployment.

Modeling and assumptions. Based on decision-makers' interviews, Forrester estimates the following for the composite organization:

- The licensing costs were developed using a customized set of use cases, professional services, and number of agents across which the solution was deployed. These costs are an aggregate based on assumptions made about the composite organization and are expected to grow by 3% annually.
- The development and maintenance costs were calculated using the same deployment costs in the previous cost category; however, ongoing solution development and maintenance would only require a single network administrator performing two hours of development and maintenance per week.

Risks. A low risk adjustment of 10% was applied because – while prices may vary over time – the scope and level of complexity for ongoing system updates that would require solution maintenance is relatively low once the system is deployed.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of nearly $3,720,000.



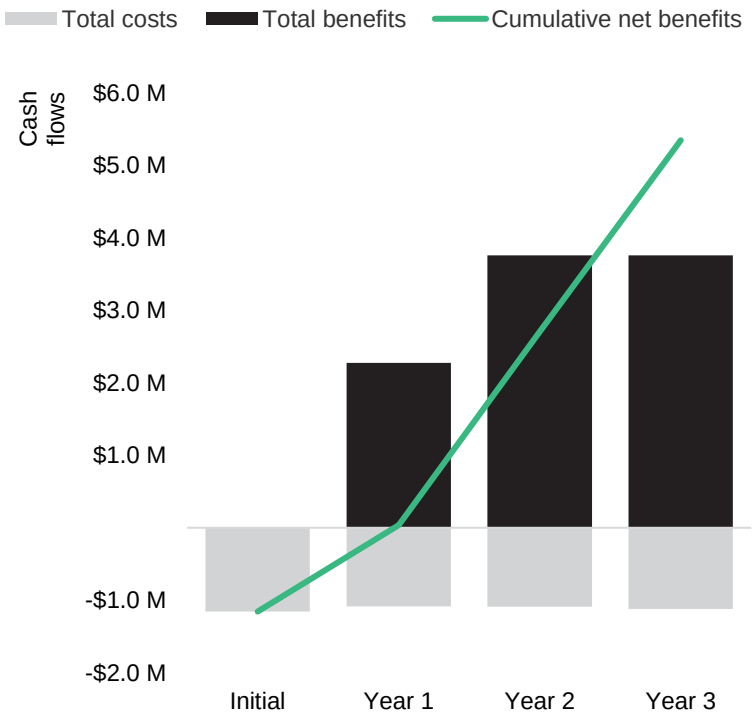
Ongoing Costs (Licensing Fees, Ongoing Solution Development And Maintenance, Etc.)

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Licensing costs*	Composite	$927,000	$954,810	$983,454	$1,012,958
G2	Hourly rate per worker	Composite	$50	$50	$50	$50
G3	Hours	Input	0	104	104	104
G4	Development and maintenance costs	G2*G3	$0	$5,200	$5,200	$5,200
Gt	Ongoing costs (licensing fees, ongoing solution development and maintenance, etc.)	G1+G4	$927,000	$960,010	$988,654	$1,018,158
	Risk adjustment	↑10%				
Gtr	Ongoing costs (licensing fees, ongoing solution development and maintenance, etc.) (risk-adjusted)		$1,019,700	$1,056,011	$1,087,520	$1,119,974
	Three-year total: $4,283,204			**Three-year present value: $3,719,939**		

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	($1,155,400)	($1,084,761)	($1,087,520)	($1,119,974)	($4,447,654)	($3,881,775)
Total benefits	$0	$2,275,722	$3,758,847	$3,758,847	$9,793,416	$7,999,401
Net benefits	($1,155,400)	$1,190,961	$2,671,327	$2,638,873	$5,345,762	$4,117,626
ROI						106%
Payback period						12 months

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

The interest rate used in cash flow analysis to account for 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] 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.

[2] Source: "Cost of a Data Breach Report 2021," Ponemon Institute, July 2021. Using the data from IBM and the Ponemon Institute report, Forrester performed an analysis of the average size of a data breach for companies with 1,000 to 5,000 persons, and the average size of a data breach for companies with 5,000 to 10,000 persons. Forrester then compared that analysis with the size of the composite organization to obtain this figure as the expected size and costs associated with a potential security exposure.

[3] Source: Ibid.

[4] These variables are representative of a culmination of assumptions made about the composite organization.


FORRESTER®