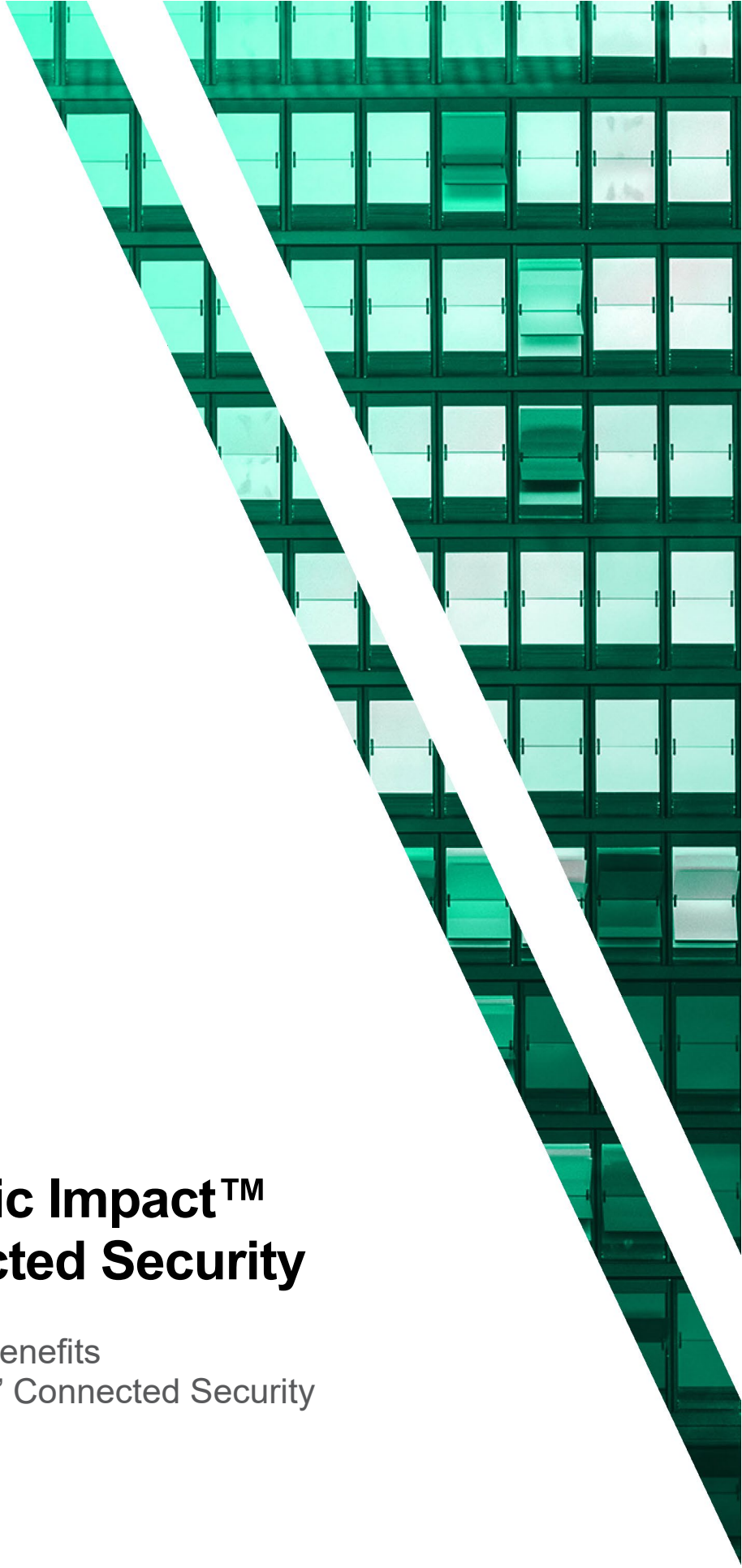
FORRESTER®



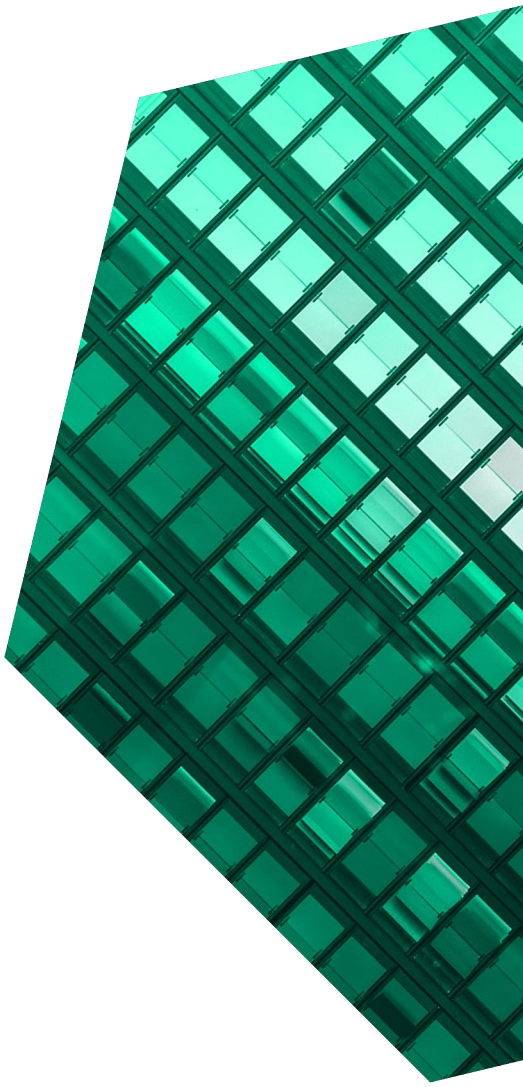
The Total Economic Impact™ Of Juniper Connected Security

Cost Savings And Business Benefits Enabled By Juniper Networks' Connected Security Strategy

JUNE 2021

Table Of Contents

Consulting Team: Casey Sirotnak
Sanitra Desai



ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

Executive Summary

> Forrester recognizes that many enterprises want to implement networking concepts, products, or technology as their networking strategy goals, yet few understand what those goals are. At best, enterprises without a clear strategy risk having a lax network that gives teams more leeway and escape routes. At worst, the network could hinder the competitiveness of the business by hampering digitalization efforts.[1]

Juniper is a full-stack security provider that offers dashboarding and tools to further streamline security operations (SecOps) while uncovering deep insights into network health and activity.

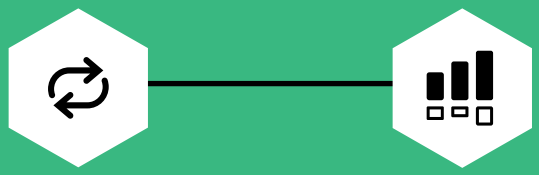
Juniper Networks commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Juniper Connected Security. The purpose of this study is to provide readers with a framework to evaluate the potential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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed an organization with experience using Juniper Connected Security. Forrester used this experience to project a three-year financial analysis.

Prior to using Juniper Connected Security, the customer had aging security equipment from a variety of vendors in place. Therefore, the legacy network security hardware was not only complicated to manage across multiple vendors and multiple different types of code, but it also lacked the necessary transparency to ensure a stable environment. These limitations led to a high level of administrative overhead that was only exacerbated by the higher risk of incidents in the prior network.

After the investment in Juniper Connected Security, the customer was able to modernize and streamline its network equipment with Juniper as a single vendor. Key results from the investment include reduced administrative overhead and having a more stable and trustworthy security environment that inspired confidence across the technology teams responsible for security operations as well as the end users/employees.

KEY STATISTICS



Return on investment (ROI)
283%

Net present value (NPV)
$657.7K

KEY FINDINGS

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

- **60% reduction in administrative overhead for security operations teams.** Security operations teams benefited from intuitive tools, dashboarding, and reporting as well as orchestration that improved network diagnostics and problem-solving efforts. Additionally, increased transparency into the network helped to create a more stable environment with fewer incidents and clearer response paths. In total,

Downtime saved per employee, annually

20 hours

these efficiencies saved the organization $354,500 over three years.

- **10% improvement to system uptime that saved employees about 20 hours of downtime each year.** Having a more secure and reliable network created with Juniper improved system performance and mitigated downtime for end users/employees. Reduced downtime for employees meant they could focus on content creation and delivery efforts that fueled the business and saved $439,700 total over three years.
- **Avoidance of $45,000 up-front capex and $35,000 annual maintenance costs.** Decommissioning aging legacy equipment saved the organization $35,000 of ongoing maintenance costs associated with that equipment each year. Additionally, because Juniper is a full-stack provider, the consolidated, up-front capex costs for hardware and saved the organization $45,000 in Year 1. The savings totaled $121,600 over three years.

Unquantified benefit. The customer identified one benefit that could not be quantified for this study: improved network confidence. Juniper provided a more stable security environment that encouraged IT teams and employees to be more innovative. IT teams experienced greater efficiencies, and they could therefore redirect their time to spinning up more modern architectures that powered business transformation. Similarly, employees no longer faced technical obstacles tied to poor system performance, and they were free to focus on delivering creative content that further enabled transformation efforts.

Costs. Risk-adjusted PV costs include:

- **Up-front and ongoing fees paid to vendors (including Juniper) and the cost of internal resource time spent on training.** Up-front costs associated with the Juniper investment included hardware fees paid to Juniper as well as implementation service fees paid to a third-party vendor. Additionally, internal resources dedicated to the ongoing maintenance and administration of the Juniper solution were required to spend about 40 hours up front getting familiar with the network components and available tooling. Ongoing training requirements were minimal and totaled 10 hours annually. The training focused on new features and extended functionalities offered by Juniper.

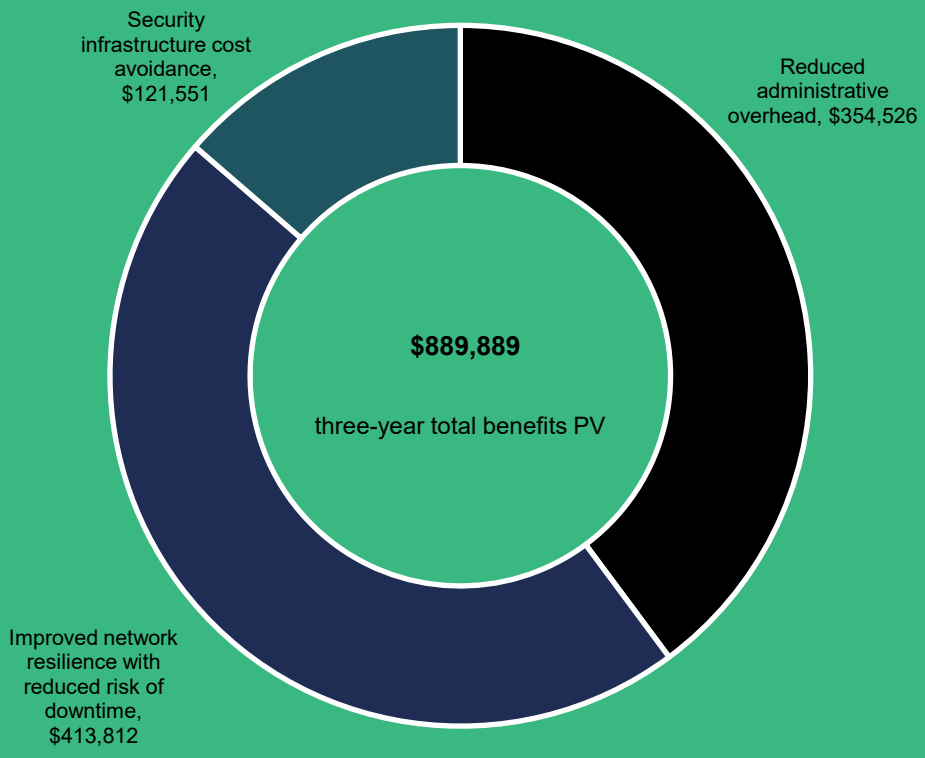
The interview and financial analysis found that this customer experiences benefits of $889,900 over three years versus costs of $232,200. This adds up to a net present value (NPV) of $657,700 and an ROI of 283%.

ROI
283%

BENEFITS PV
$889.9K

NPV
$657.7K

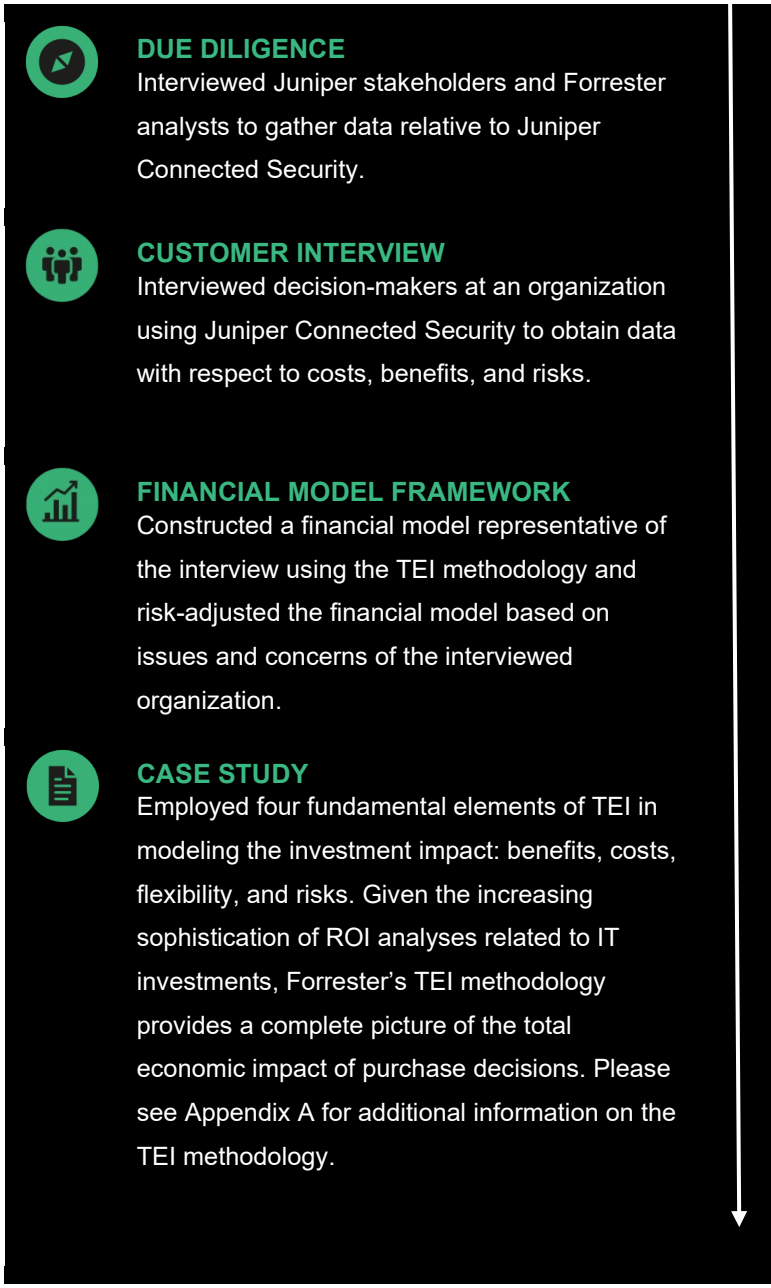
Benefits (Three-Year)



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 Juniper Connected Security.

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



The Juniper Connected Security Customer Journey

Drivers leading to the Juniper Connected Security investment

INTERVIEWED ORGANIZATION

Forrester interviewed a Juniper Connected Security customer with the following characteristics:

- It's a million-dollar multimedia organization.
- A team of two FTE is currently responsible for internal network operations.
- A driving factor for this investment was the business benefit associated with removing technical barriers and fostering a creative and collaborative environment for the 200 employees who facilitate content creation.

"The funny thing about it for me was just the deafening silence from a security standpoint of the existing tools. I would say it was very black box. We did not have any insight into what was happening on the internal network with [legacy] tools."
Director of IT, multimedia

"We wanted something [for our security network] that was a bit more modern in its approach — something that was ideally a full stack so that it would limit what we needed to learn from a new system and so we could reduce the administrative overhead on daily network operations and add changes. The older equipment was of varying generations, so [each piece of equipment] had different code bases running on it."
Director of IT, multimedia

KEY CHALLENGES

Prior to the investment in Juniper, the interviewed organization had aging equipment from various vendors constituting its security network.

As such, the organization struggled with common challenges, including:

- **Heightened administrative overhead required of security operations teams.** Aging equipment from various providers required security operations teams to work with different types of code and to interact with many stakeholders to perform any network diagnostics or to solve problems. Additionally, legacy equipment lacked the tooling, dashboarding, and/or reporting capabilities utilized in modern equipment to provide necessary transparency into the network. As a result, the organization dedicated a lot of expensive resource time to security administration.

- **Restricted resources in terms of availability, level, and capacity.** The resources dedicated to security administration were high-level resources with a wide range of responsibilities that included network administration. The organization operated with a lean team, and decision-makers did not have the ability or the desire to add discrete resources or resource time to such administrative tasks.
- **The opacity of legacy networks, which heightened the risk of security incidents that may have gone unnoticed.** The legacy equipment provided limited views into the health or activity of the network. This prompted a lack of confidence in the security of the network as operations teams had very little insight into the level of threat or the volume of potential incidents at any given point in time. Therefore, the organization was more vulnerable to incidents and the severity of their downstream impacts.

"I'm a jack-of-all-trades and master of none, and I have a very lean team. So, the legacy equipment was aging, and there was no effective lifespan left on the equipment. It was going into service end of life, but more than that, it was from a different era of networking. [That means] there was more uplift from an administrative standpoint for us in using the old equipment. It was always a hassle and a pain to have to make any changes on the network."
Director of IT, multimedia

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewed organization was moving physical office locations. Therefore, decision-makers were presented with an opportunity to make a choice about the future of the organization's network security provider.

The director of IT said: "We took the opportunity [of the office move] to upgrade and change our core networking operations from some rather old equipment in our old office space. Some of our legacy equipment was seven, eight, or even 10 years old at that point. So, the impetus for change was the office move. We also needed to be able to stand up a network in the new office space independent of the existing office space."

As such, decision-makers chose to decommission the organization's legacy equipment and start over with a new solution that could:

- Modernize the network infrastructure and streamline providers by offering full-stack capabilities.
- Migrate to the new physical office location with zero downtime and minimal impact to employees.
- Reduce the administrative overhead through intuitive tools and orchestration that provided greater network insights and a generally more stable environment.

After evaluating multiple vendors, the organization chose Juniper Connected Security and began deployment. Interviewees said the following:

- The interviewed organization was able to build its security network from the ground up with Juniper in its new physical office location.
- Because Juniper is a full stack provider, it centralized the stacks that powered the network for the entire office and greatly reduced the number of access points.

- Additionally, Juniper instituted redundancies across the organization's network that did not exist in its legacy environment through dual firewalls, dual fiber switches, and dual management across an employee campus and a data center.

We chose Juniper because it presented a really compelling case for what it could provide us, particularly from an administrative standpoint and being able to have a single operating system across all of the devices with [the Junos operating system]. On top of that, with Junos, we had a window into our networks that we never had before with its web interface that would shorten the learning curve.

— Director of IT, multimedia

Analysis Of Benefits

Quantified benefit data

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Reduced administrative overhead	$142,560	$142,560	$142,560	$427,680	$354,526
Btr	Improved network resilience with reduced risk of downtime	$166,400	$166,400	$166,400	$499,200	$413,812
Ctr	Security infrastructure cost avoidance	$76,000	$33,250	$33,250	$142,500	$121,551
	Total benefits (risk-adjusted)	$384,960	$342,210	$342,210	$1,069,380	$889,889

REDUCED ADMINISTRATIVE OVERHEAD

Evidence and data. The interviewed organization had a lean team of high-level resources that was responsible for a wide breadth of activities, including network administration. The legacy environment consisted of aging equipment from various vendors that was not only more fragile and more opaque, but it also required esoteric coding and vendor-specific knowledge across many vendors to make changes or solve problems when necessary. Juniper Connected Security, managed by Juniper Security Director, provided a modern network security infrastructure complete with dashboards and intuitive tools and orchestration that lent more transparency and efficiencies to its' administration and created a more stable environment. As a result, the organization greatly reduced the overhead required for network administration.

- The director of IT for the organization explained how various efficiencies provided by Juniper translated into a reduction in time spent on network administration. They said: "Previously, I would say one FTE spent probably 50% of their time on networking issues at the old office, and I probably did the same 10% or 15% of the time. But the overall effect was that we had two senior resources working on the network. We're not cheap workers. [With Juniper,] we have saved 30% to 35% of our time dealing with network security and not having to worry about network connectivity issues."

  The organization was also able to reduce the number of discrete resources responsible for network and security administration. The interviewee said: "The administrative overhead is far lower than it was before. We're down one person [in terms of head count compared to what was required in our previous environment], and we're still able to manage what we have to manage around the network because it has become much simpler to operate."

- The organization attributed many of the efficiencies gained with the Juniper network to intuitive Juniper Security Director management and orchestration tools and views. The Junos dashboard allowed the interviewee and their team to maintain their lean numbers and feel confident about their network security without becoming dedicated experts in the area. The interviewee stated: "The administrative overhead [we experienced in our legacy environment] was something that we just had to get under control.

In our new facility, we wanted to be able to 'fish for ourselves.' So, we needed to be able to understand our network and its configuration as quickly as possible. We relied very heavily on [the Junos web interface] at the beginning, which worked like training wheels. As someone who has not been a network administrator my whole life, it was a great thing to be able to get in there via a web browser and see something and visualize it outside of the CLI (command-line interface)."

- Juniper enabled the interviewed organization to consolidate its previously disparate equipment. The new ecosystem enabled faster diagnostics and easier problem-solving efforts from the increased transparency that the Juniper network provided and because the organization did not need to deal with multiple codes and vendors. Having more transparency meant having more clarity around the types of incidents or alarms that required action. The interviewee stated: "There were network connectivity problems, and because the administration of our older systems was sort of fragmented and fractured across multiple different types of devices and generations of devices, it meant quite a lot of pain in discovering the source of a breach. And we are just talking about discovery at that point. We're not even into remediation. Now, with Juniper Connected Security, I feel like it's easier for me to spot false alarms or to identify weird behavior that doesn't necessarily require action."
- The Juniper network and associated tools created an overall more stable security environment that inherently reduced the amount of administration required. The interviewee stated: "One of the reasons why it's so little [administrative overhead] is because we've gotten to a level where our needs are met. We have optimized what we can optimize for our internal networking situation. We have redesigned our VLANs (virtual local area networks) and our site-to-site connections. Since then, the network has been secure in a rock-solid sort of way."

Modeling and assumptions. To calculate the reduced administrative overhead, Forrester assumes the following:

- The legacy environment required 3 FTE for administration at varying degrees of dedication. Once transitioned to the Juniper environment, the organization could reassign 1 FTE and mitigate the time spent for the remaining 2 FTE.
- The organization immediately experienced 60% efficiencies for SecOps FTE in Year 1. These efficiencies remained consistent across the three-year investment due to the stability of the security network.
- SecOps resources have an average annual salary of $110,000.
- 80% of the efficiencies gained through tooling, network transparency, and stability were repurposed for value-add work.

"I think the main benefit behind what we have is the tools themselves and the visibility they provide into the network, which gives us the ability from an administrative standpoint to use and understand who and what is on the network and to enforce policies across multiple environments."
Director of IT, multimedia

Risks. Reduced administrative overhead may vary depending on the following:

- The state of the legacy network environment (e.g., age, vendor, etc.) and the volume of SecOps resources dedicated to its administration.
- The level of a resource required to participate in network administration and their associated annual salary.
- The variance of salaries by region.
- The percent of productivity captured by SecOps teams for more value-add work (which may also depend on the technical and business initiatives running in parallel).

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $354,526.

Reduced Administrative Overhead

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	SecOps FTE responsible for network administration before Juniper Connected Security	Interview	3	3	3
A2	Reduced administrative overhead with Juniper Connected Security	Interview	60%	60%	60%
A3	SecOps FTE average annual salary	Assumption	$110,000	$110,000	$110,000
A4	Productivity capture percentage	Assumption	80%	80%	80%
At	Reduced administrative overhead	A1*A2*A3*A4	$158,400	$158,400	$158,400
	Risk adjustment	↓10%			
Atr	Reduced administrative overhead (risk-adjusted)		$142,560	$142,560	$142,560
	Three-year total: $427,680			**Three-year present value: $354,526**	

IMPROVED NETWORK RESILIENCE WITH REDUCED RISK OF DOWNTIME

Evidence and data. Previously, the interviewed organization experienced incidents and outages that impacted employees in terms of downtime. The level of impact cultivated a level of distrust between the employees and their network foundation that distracted from the creative and collaborative work they were responsible for. With Juniper, the organization experienced far less downtime for employees, allowing them to focus on delivering media content to the customer base without technical disruptions.

- The legacy equipment that supported network security was very “black box” and difficult to navigate and manage. Therefore, the organization experienced an elevated risk of severe events. Juniper’s increased transparency and improved network stability reduced the possibility of a catastrophic event. The interviewee said: “If we just imagine for a second what a security event might have looked like with our legacy equipment, if anything, it would have

had to have exhibited itself in such a catastrophic way for us to be aware of it at the time. That means that there could have been a significant security breach that would have caused network downtime. So, the possibility for a catastrophic failure was very high in our previous environment. With Juniper, I feel much more comfortable that these kinds of events are preventable, due largely to the visibility we have into the system now."

- The issues experienced in the previous environment largely manifested as outages that impacted employees in terms of downtime, which left the environment vulnerable to attack. The interviewee stated: "In our previous environment, we had a lot of switch connectivity issues. There were also a lot of port interface issues and connectivity VLAN issues, updates, upgrades, and downtime related to them. I don't think we ever managed to get anything on its most recent version. Therefore, our update schedule was rolling, which would cause rolling outages that resulted in downtime for employees and risk to our environment, despite our best efforts to perform updates during 'off' or 'nonwork' times."
- With Juniper, network performance greatly improved, therefore reducing the impact on employees. The interviewee said: "With the Juniper equipment, we haven't had any network outages or compromised events. In fact, my delivery rates from over the last three years have been some of the best of my career. They are very easily in the 99% range for just about everything I have — network included. Before, we were in the high 80s or low 90s. So, it's been about a 10% improvement."
- Employees also benefited from improved network resilience in terms of elevated levels of trust. Without technical disruptions, employees focused on delivering content to consumers. The interviewee said the impact was "the difference between the user feeling like there's a solid and secure foundation behind them that is immutable versus something that is chaotic and disruptive and requires aggressive complaint."

Modeling and assumptions. To calculate improved network resilience with reduced risk of downtime, Forrester assumes the following:

- The organization has 200 employees focused on content creation who would be impacted by potential downtime events.
- The legacy environment experienced 89% system availability. This left 11% of the time (or 229 hours annually) vulnerable to catastrophic downtime events that could impact employees.
- With Juniper, the organization improved its system performance by 10%, thereby reducing the risk of catastrophic downtime annually.
- Not all downtime events impact employees. Forrester assumes that 10% of these events are catastrophic to the point of employee downtime.
- Downtime costs per user (or employee) of $50 accounts for both employee hourly rates – given that employees have a restricted capacity to work during system downtime – as well as impact to the business. System downtime also impacts the ability of those employees to deliver content to consumers, thereby diminishing opportunity costs.

Risks. Improved network resilience with reduced risk of downtime will vary depending on the following:

- The size of the organization in terms of employee count.
- The level of system availability achieved in the legacy environment as well as the improvement experienced with Juniper.
- The percentage of potential downtime events that impact employees.

- The average hourly rate for employees, which varies across industry, region, job type, and job level. Additionally, the nature of the business conducted by these employees will impact any associated opportunity costs lost during downtime. More customer-facing work will have a higher impact on opportunity costs.

To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $413,812.

Improved Network Resilience With Reduced Risk Of Downtime

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Number of users/employees	Interview	200	200	200
B2	Hours of downtime caused by network incidents per year before Juniper	Assumption	229	229	229
B3	Hours of downtime caused by network incidents per year with Juniper	Assumption	21	21	21
B4	Volume of network incidents with material impact to employees	Assumption	10%	10%	10%
B5	Downtime cost per user	Assumption	$50	$50	$50
Bt	Improved network resilience with reduced risk of downtime	B1*((B2-B3)*B4)*B5	$208,000	$208,000	$208,000
	Risk adjustment	↓20%			
Btr	Improved network resilience with reduced risk of downtime (risk-adjusted)		$166,400	$166,400	$166,400
	Three-year total: $499,200			**Three-year present value: $413,812**	

SECURITY INFRASTRUCTURE COST AVOIDANCE

Evidence and data. The interviewed organization experienced cost avoidances because decision-makers chose to decommission legacy equipment and streamline to a new, single vendor for security infrastructure. The legacy equipment was aging and, therefore, there were hefty annual maintenance costs associated with it. But the organization avoided those costs when it moved to Juniper for security infrastructure. Additionally, because Juniper is a full-stack provider, it had more control over up-front hardware costs, which initially saved the organization capex expenditure.

- The director of IT at the organization explained the cost avoidances in more detail. They said:

  "When I talk about cost savings, I'm really talking about the purchase cost as well as an element of total cost of ownership involved because of the support contracts and how we negotiate those. From a purchase perspective, it was capex savings on hardware and equipment. Juniper presented the best offer because it was able to package everything together — being a full-stack provider and all. That gave it a lot of leverage on pricing."

- The interviewee estimated that the up-front cost savings for the capital purchase and integration setup and configuration with Juniper were in the range of $40,000 to $45,000. Additionally, the interviewee indicated that their organization avoided about $35,000 a year on maintenance

Up-front capex cost savings

$45K

Ongoing maintenance cost avoidance

$35K annually

costs that were associated with legacy equipment.

Modeling and assumptions. To calculate security infrastructure cost avoidance, Forrester assumes the following:

- Juniper costs $45,000 less on up-front capex expenditure for hardware than the alternative solution.
- The legacy solution required $35,000 of annual maintenance costs that are avoided with the Juniper solution.

Risks. Security infrastructure cost avoidance may vary depending on the following:

- The maintenance requirements of the legacy solution per the annual contract.
- The alternative solutions considered (which will impact up-front capex savings).

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $121,600.

Security Infrastructure Cost Avoidance

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Up-front capex expenditure avoided with Juniper Connected Security	Interview	$45,000	$0	$0
C2	Avoided maintenance cost of legacy solution	Interview	$35,000	$35,000	$35,000
Ct	Security infrastructure cost avoidance	C1+C2	$80,000	$35,000	$35,000
	Risk adjustment	↓5%			
Ctr	Security infrastructure cost avoidance (risk-adjusted)		$76,000	$33,250	$33,250
	Three-year total: $142,500		**Three-year present value: $121,551**		

UNQUANTIFIED BENEFITS

Additional benefits that the customer experienced but was not able to quantify include:

- **IT teams are able to explore more complicated and modern architectures.**

Juniper's Connected Security solution greatly reduced the overhead associated with network and security administration while also improving the stability of the environment. As a result, IT teams had more time to focus on innovative initiatives, and they had more confidence to

introduce complicated architectures like hybrid cloud to the environment.

- **Employees can focus on content creation and collaboration.** Having more network stability meant that technology was no longer in the way of employees on a regular basis. Therefore, they could focus on maintaining a collaborative and creative production environment that was critical to business success.

"Our previous security environment consisted of different levels of delicately balanced equipment. With Juniper, we have a strong underlying foundation made up of a single stack with security tooling built in. The Juniper network configuration helped us to better understand the capabilities of our security equipment and tools, which allowed us to feel confident expanding into new and different technical areas."
Director of IT, multimedia

"I've had users lose confidence in the systems that we've run before, and bringing [those systems] back from the brink of death becomes a real marketing/PR task with users, rather than a technology task. It's a trust factor, and that is the difference between where we were versus where we are now. We've reached a sweet spot — sort of a unicorn zone."
Director of IT, multimedia

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Juniper's Connected Security solution and later realize additional uses and business opportunities.

One such use includes enabling better business transformation. With the investment in Juniper Connected Security, IT teams experimented with more complex, flexible, and modern architectures like hybrid cloud, and employees were not impacted by technical issues. As such, the organization focused energy on business transformation initiatives that were empowered by the technical foundation Juniper provided; not hindered by it. Therefore, decision-makers anticipate more innovations powered by the organization's newfound technical freedom and flexibility.

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

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Dtr	Up-front and ongoing fees paid to vendors	$0	$218,500	$17,250	$17,250	$253,000	$225,853
Etr	Internal resource time spent on onboarding and training	$0	$4,865	$1,216	$1,216	$7,298	$6,342
	Total costs (risk-adjusted)	$0	$223,365	$18,466	$18,466	$260,298	$232,195

UP-FRONT AND ONGOING FEES PAID TO VENDORS

Evidence and data. The interviewed customer paid upfront fees to Juniper for its Connected Security hardware and software along with implementation. Additionally, the organization negotiated a maintenance contract with Juniper for ongoing maintenance and support.

Modeling and assumptions. To calculate the up-front and ongoing fees paid to vendors, Forrester assumes the following:

- Up-front costs include hardware and software fees paid directly to Juniper, as well as implementation fees that are paid through Juniper to a third-party vendor for implementation services, including required integrations. The organization incurred hardware, software, and implementation costs in Year 1.
- Implementation spanned the course of a single weekend and cost the organization a total of $175,000.
- Ongoing costs are indicative of the maintenance and support contract between Juniper and the interviewed customer. The costs total $15,000 annually.

Risks. The up-front and ongoing fees paid to vendors may vary depending on the following:

- The size and scope of the Juniper investment in terms of the hardware and software required to run the associated security network.
- Expectations about the implementation timeline.
- The maintenance contract negotiated between Juniper and the customer in terms of years of covered costs under the up-front fees and the value of ongoing maintenance not covered by the up-front fees.

To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV of $225,853.

Up-Front And Ongoing Fees Paid To Vendors						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Up-front hardware and project costs paid to Juniper and third-party implementation partners	Interview	$0	$175,000	$0	$0
D2	Ongoing fees paid to Juniper	Interview	$0	$15,000	$15,000	$15,000
Dt	Up-front and ongoing fees paid to vendors	D1+D2	$0	$190,000	$15,000	$15,000
	Risk adjustment	↑15%				
Dtr	Up-front and ongoing fees paid to vendors (risk-adjusted)		$0	$218,500	$17,250	$17,250
	Three-year total: $253,000			**Three-year present value: $225,853**		

INTERNAL RESOURCE TIME SPENT ON ONBOARDING AND TRAINING

Evidence and data. The interviewed customer said that in addition to paying fees to Juniper and other outside vendors, the organization also dedicated resource time to onboarding and training associated with the Juniper Connected Security solution.

Modeling and assumptions. To calculate internal resource time spent on onboarding and training, Forrester assumes the following:

- The organization has a lean team of two security operations FTE dedicated to the ongoing maintenance and administration of the Juniper Connected Security solution.
- The SecOps FTE initially spent 40 hours of training time to get fully onboarded to the Juniper system and to learn how to effectively operate the tools.
- In subsequent years, a very light training effort is required to account for new features and functionalities. This totals 10 hours annually.

Risks. Internal resource time spent on onboarding and training may vary depending on the following:

- The number of SecOps FTE and their dedication to the Juniper Connected Security solution.
- Familiarity with security network hardware and software.
- The size and scope of the Juniper investment.

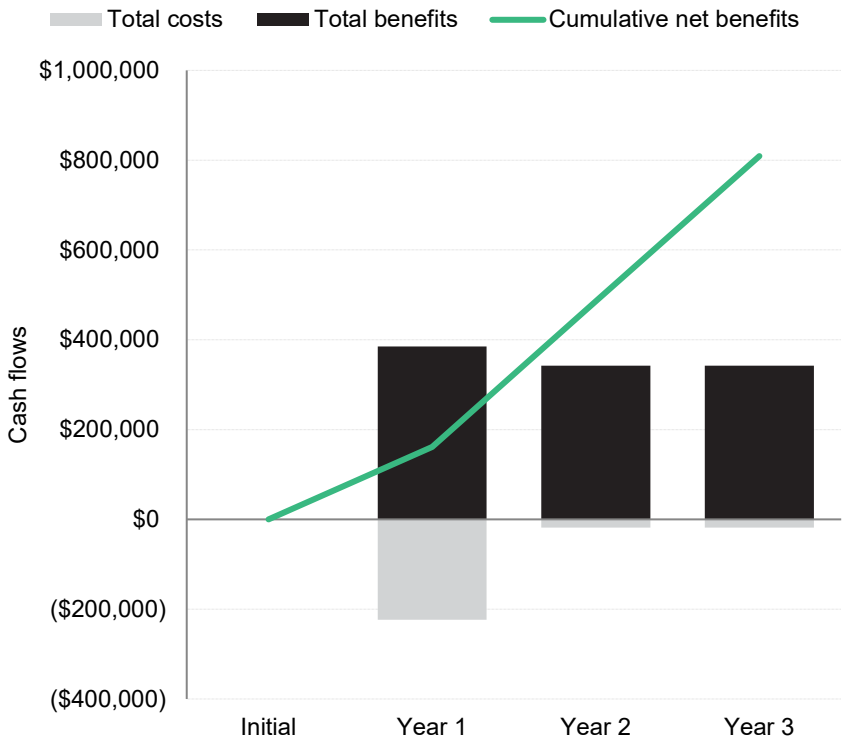
To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV of $6,342.

Internal Resource Time Spent On Onboarding And Training						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	FTE responsible for ongoing maintenance and administration of Juniper	Interview	0	2	2	2
E2	Time required for onboarding and training (hours)	Interview	0	40	10	10
E3	Average hourly rate for SecOps FTE	Assumption	$0	$53	$53	$53
Et	Internal resource time spent on onboarding and training	E1*E2*E3	$0	$4,231	$1,058	$1,058
	Risk adjustment	↑15%				
Etr	Internal resource time spent on onboarding and training (risk-adjusted)		$0	$4,865	$1,216	$1,216
	Three-year total: $7,298			**Three-year present value: $6,342**		

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 and NPV for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, and NPV 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	$0	($223,365)	($18,466)	($18,466)	($260,298)	($232,195)
Total benefits	$0	$384,960	$342,210	$342,210	$1,069,380	$889,889
Net benefits	$0	$161,595	$323,744	$323,744	$809,082	$657,694
ROI						283%

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

PAYBACK PERIOD

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

Appendix B: Endnotes

[1] Source: “Now Tech: Virtual Network Infrastructure Switching Fabric, Q2 2020,” Forrester Research, Inc., April 22, 2020.


FORRESTER®