

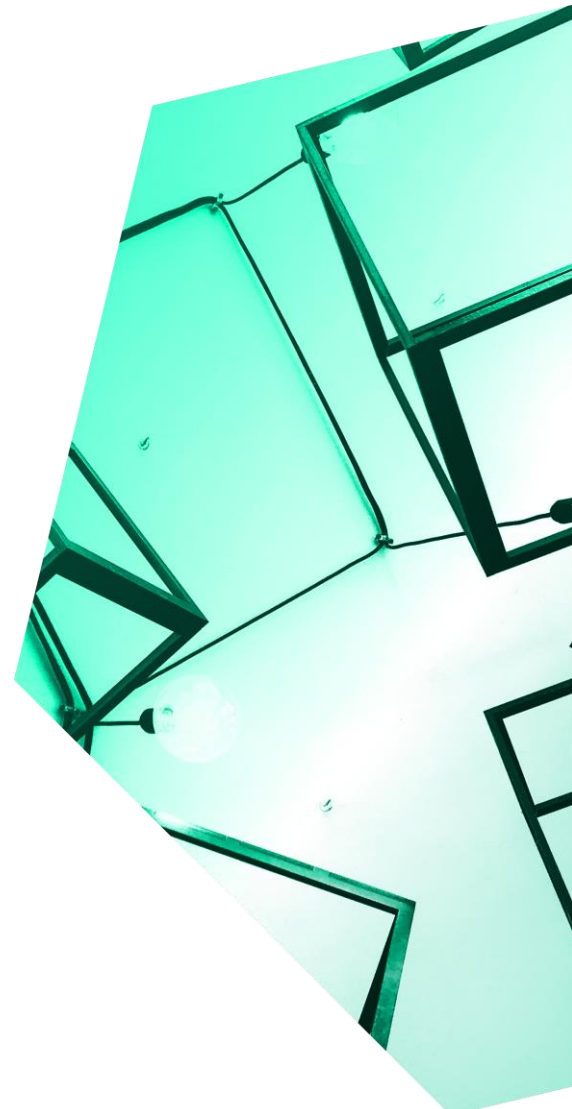
The Partner Opportunity For ConnectWise Cybersecurity Management

A Total Economic Impact™ Partner Opportunity Analysis

FEBRUARY 2023

Table Of Contents

- Executive Summary1**
- The ConnectWise Cybersecurity Management Partner Journey6**
 - Partner Goals, Challenges, And Drivers6
 - Selecting The Right Partner Program7
 - Composite Organization.....8
- Analysis Of Partner Revenue Streams9**
 - Cybersecurity Managed Services Annual Gross Profit9
 - Unquantified Benefits12
 - Flexibility.....13
- Analysis Of Partner Investments14**
 - Cybersecurity Managed Services Practice Investments14
- Financial Summary16**
- Appendix A: Total Economic Impact17**
- Appendix B: Endnotes18**



ABOUT FORRESTER CONSULTING

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

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

Executive Summary

Now more than ever, cybersecurity is a critical focus area for businesses globally. “Instilling and maintaining trust with customers, employees, and partners is a business imperative ... when geopolitical events and technology disruption continue to fuel a highly sophisticated and evolving threat landscape.”¹ As companies seek to improve security postures and reduce risk, there is an opportunity for technology solution providers to build and grow revenue-generating cybersecurity practices to serve clients.

ConnectWise provides information technology (IT) service providers with the support, services, and solutions they need to succeed. These solutions include ConnectWise Business Management, ConnectWise Unified Monitoring & Management, and [ConnectWise Cybersecurity Management](#).

In particular, Cybersecurity Management helps IT service providers protect clients with security information and event management (SIEM), managed detection and response (MDR), security operations center as a service (SOCaaS), and more. Furthermore, ConnectWise provides the resources, community, and support organizations need to build security practices and revenue streams with the [ConnectWise Partner Program for Cybersecurity](#).

ConnectWise commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study to examine the potential business opportunity and return on investment (ROI) partners may realize by building and scaling a cybersecurity practice with ConnectWise Cybersecurity Management solutions.² The purpose of this study is to provide potential and

KEY STATISTICS



Price per seat increase
65%



Gross margin (Year 3)
55%

existing partners with a framework to evaluate the potential business opportunity associated with using ConnectWise Cybersecurity Management solutions to service clients as part of the ConnectWise partner ecosystem.

To better understand the revenue streams, investments, and risks associated with a Cybersecurity Management practice, Forrester interviewed four representatives of existing Cybersecurity Management partners with experience collaborating with ConnectWise to build or innovate and ultimately sell and scale their practices. These partners are managed service providers (MSPs) of varying sizes in North America, Europe, and Australia that generate revenues ranging from \$950,000 to \$45 million and have workforces of between five and 150 team members.

To illustrate the financial impact and subsequent partner business opportunity for Cybersecurity Management partners, Forrester aggregated the

Higher new customer
growth rate

43%



characteristics of these interviewees and combined the results into a single **composite organization** that is an MSP that generates between \$3 million and \$5 million in revenue and has 20 to 30 employees.

KEY FINDINGS

Revenue opportunities. The composite partner organization captures the following revenue stream, which is representative of those experienced by interviewees' organizations:

- **Annual gross profit from cybersecurity-managed services worth \$1.90 million.** With the guidance and extensive support of ConnectWise, the composite partner utilizes Cybersecurity Management solutions to enhance its preexisting managed services offering, and this yields better value for its clients. This enables the composite partner to grow its customer base,

were able to eliminate low-value tasks and instead focus on revenue-creating tasks to scale and grow their practices.

- **Significant 24/7 security operations center (SOC) savings.** In particular, the interviewed decision-makers said it is cost-prohibitive to build and operate SOCs without ConnectWise.
- **Cyber insurance support and benefits.** Interviewees helped their organizations' clients prepare for and benefit from cyber insurance.
- **Support, collaboration, and relationships.** Interviewees said their organizations' ConnectWise partnerships extended well beyond the solutions and services. They value the community, collaboration, and support to package, implement, market, and sell a cybersecurity service and being able to bring ConnectWise experts into client meetings.

Investments. Beyond the costs of service delivery and Cybersecurity Management solutions, which are embedded in the gross margin calculations of the revenue stream, partners also invested in:

- **Research and development investments of \$41,000.** To build, maintain, and improve its new business, the composite partner allots 1% of practice revenue. Over the three-year analysis period, this investment contributes 10.5% of the composite's total operating expenses.
- **Training investments of \$102,000.** The composite partner commits to training its sales and delivery staff. Over the three-year analysis period, this investment contributes 26.1% of the composite's total operating expenses.
- **Sales and marketing investments of \$177,000.** The composite partner allocates 5% of practice revenue to sales and marketing. Over the three-year analysis period, this investment contributes 45.3% of the composite's total operating expenses.

Preexisting customer expansion rate per year

25%



charge a premium, and increase its gross margin.

Key outcomes. Benefits that provide value for the composite partner organization but are not quantified for this study include:

- **Superior client outcomes, including improved security posture and lowered risk.** Interviewees said their organizations' clients benefitted from Cybersecurity Management solutions and that their organizations were able to respond to ransomware attacks in minutes rather than hours.
- **Improved, scaled, automated, and focused operations.** Interviewees said their organizations

- **General and administrative investments of \$71,000.** For daily operations, the composite partner allocates 2% of its revenue. Over the three-year analysis period, this investment contributes 18.1% of the composite’s total operating expenses.

Net results. The representative interviews and financial analysis found that a composite partner experiences total present value (PV) gross profits of \$1.90 million over three years versus investments and overhead expenses of \$391,000, adding up to a net present value (NPV) of \$1.51 million and an ROI of 386%.

Cybersecurity Management Partner Pro Forma Revenue And Margin Opportunity: Three-Year Analysis (USD)

Ref.	Metric	Source	Year 1	Year 2	Year 3
PL1	Cybersecurity managed services annual revenue	A13	\$546,000	\$1,384,500	\$2,527,200
PL2	Total revenue	PL1	\$546,000	\$1,384,500	\$2,527,200
PL3	Total gross profit	At	\$273,000	\$733,785	\$1,389,960
PL4	Total gross margin	PL3/PL2	50%	53%	55%
PL5	Research and development investments	B2	\$10,920	\$13,845	\$25,272
PL6	Training investments	B3	\$27,300	\$34,613	\$63,180
PL7	Sales and marketing investments	B4	\$27,300	\$69,225	\$126,360
PL8	General and administrative investments	B5	\$10,920	\$27,690	\$50,544
PL9	Total operating expenses	PL5+PL6+PL7+PL8	\$76,440	\$145,373	\$265,356
PL10	Operating income	PL3-PL9	\$196,560	\$588,412	\$1,124,604
PL11	Operating margin	PL10/PL2	36%	42%	45%

“To offer all we do now [with ConnectWise] along with the relationships is phenomenal. It puts us on the same playing field as larger MSPs. We can do it as well as them.”

— CEO, Australian MSP for SMBs



ROI
386%

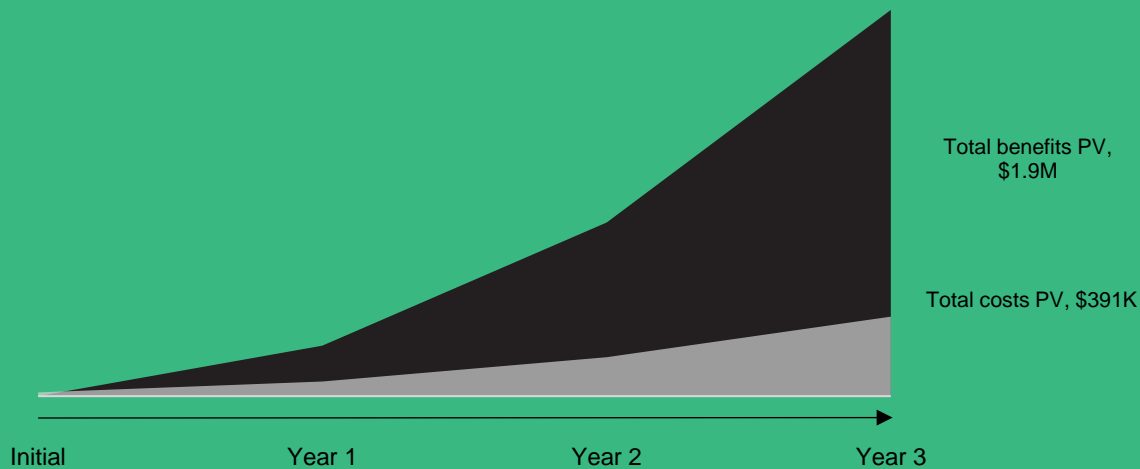


GROSS MARGIN
55% in Year 3



OPERATING MARGIN
45% in Year 3

Financial Summary



“There was no way we could deliver what we’re delivering without increasing headcount significantly. ... The training, support, and price is a winning combination.”

— Managing director, European MSP for SMBs

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those partners considering building and growing a ConnectWise Cybersecurity Management practice.

The objective of the framework is to identify the revenue streams, investments, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the holistic opportunity for partners building and growing a ConnectWise Cybersecurity Management practice.

DISCLOSURES

Readers should be aware of the following:

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

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

ConnectWise reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

ConnectWise provided the partner names for the interviews but did not participate in the interviews.



DUE DILIGENCE

Interviewed ConnectWise stakeholders and Forrester analysts to gather data relative to ConnectWise Cybersecurity Management.



INTERVIEWS

Interviewed four representatives at partner organizations with existing ConnectWise Cybersecurity Management practices to obtain data with respect to costs, benefits, and risks.



COMPOSITE ORGANIZATION

Designed a composite partner 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 interviewees.



CASE STUDY

Employed four fundamental elements of TEI in modeling the impact of a Cybersecurity Management practice: revenue, investments, 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 investment and partnership decisions. Please see Appendix A for additional information on the TEI methodology.

The ConnectWise Cybersecurity Management Partner Journey

■ Drivers leading to the Cybersecurity Management practice investment

Interviews				
Role	Organization type	Region	Revenue	Employees
General manager of IT services	MSP and general IT services	Headquartered in North America	\$45M+	150
Managing director	MSP for SMBs with 10 to 280 employees	Headquartered in Europe	\$3.5M+ (£3M+)	30
Business owner	MSP	Headquartered in Australia	\$3M+ (\$4.5M+ AUD)	20
CEO	MSP for SMBs	Headquartered in North America	\$950,000	5

PARTNER GOALS, CHALLENGES, AND DRIVERS

Partners were diverse in size, background, functional and vertical specializations, type, and degree of engagement with ConnectWise. They partnered with ConnectWise to build and scale their Cybersecurity Management businesses for many reasons, including:

- **No formalized security offerings.** Before using ConnectWise Cybersecurity Management solutions, most interviewees' organizations did not have formal or sophisticated security offerings. Interviewees said it would be capitally intensive and risky to build out self-managed security offerings and that their organizations often initially lacked expertise, insight, and understanding of security risk management.
- **Basic security coverage with an antivirus platform.** The managing director of a European MSP for SMBs said: "We were using a normal antivirus platform. We were keeping our clients in line with Cyber Essentials and having the Cyber Essentials certified by a third party. We were rolling in a spam filter. ... The way the climate is going and the cybersecurity landscape, it means that's not suitable anymore."

"We didn't have any formalized security offering two years ago. We did some security tasks, but we didn't have an offering. [ConnectWise] is 24/7 eyes on the glass so that we can focus on the more strategic items."

General manager of IT services, North American MSP and general IT services organization

- **Existing relationships.** The interviewees indicated that their organizations were already customers of ConnectWise and used its Unified Monitoring & Management and Business Management solutions to serve clients. The business owner of an Australian MSP said, "We've developed a good relationship with ConnectWise over five [or] six years."

SELECTING THE RIGHT PARTNER PROGRAM

In choosing a partner and platform around which to build their cybersecurity managed service, interviewees emphasized the following factors:

- **High quality, competitive tools, and services.** Decision-makers said that with Cybersecurity Management, ConnectWise offered the leading solutions and services their organizations needed to serve clients well and to expand their managed-service offerings. Furthermore, interviewees said ConnectWise helped them secure their organizations' environments with security checklist evaluations and it taught them best practices on how to similarly service clients.

- **Security reassurance due to 24/7 access to SOCaaS.** One key criterion the interviewees referenced when they chose ConnectWise was having access to 24/7 SOCaaS with Cybersecurity Management. They indicated that their companies would have had to make significant investments to offer something similar. Therefore, they desired this feature to help their organizations offer the capabilities of larger MSPs.
- **Revenue improvements by reaching more and larger businesses.** Similarly, interviewees said their organizations saw being able to offer capable cybersecurity managed services as an opportunity to gain business with larger organizations and increase deal sizes.
- **Ability to leverage ConnectWise marketing and sales expertise with clients.** Interviewees said that when selecting their organizations' partner programs, they valued the opportunity to collaborate with ConnectWise for marketing, sales, funding, and other support.

“We’ve got this great solution. We’ve partnered with ConnectWise, [which is] a huge international company. [It has] ... live human beings assessing logs, looking for breaches, and hunting for cyberbreaches [24/7]. That’s great.”

Business owner, Australian MSP

- **Familiarity with the ConnectWise ecosystem.** Because the interviewees' organizations were already working with ConnectWise, they were familiar with the opportunities. Thus, they chose to extend their partnerships and enhance their practices with Cybersecurity Management.
- **Favorable pricing to improve margins.** Beyond the technical capabilities of the Cybersecurity Management solutions and the ConnectWise partnership, interviewees noted how the pricing was favorable and could improve their organizations' margins.

“[ConnectWise] does marketing events with us, [talks] to our customers, and [does] presentations, so [there’s] a lot of value. We did look at other security partners. They didn’t have the people behind [them]. They were just selling [solutions].”

General manager of IT services, North American MSP and general IT services organization

- **Ability to free up the organizations' own engineers to work on billable hours, proactive projects, and revenue-generating tasks.**

Interviewees emphasized that their organizations saw using ConnectWise Cybersecurity Management solutions and services in connection with professional-services automation (PSA), remote monitoring and management (RMM), and ConnectWise Automate as an opportunity to focus on more pertinent and value-generating activities.

COMPOSITE ORGANIZATION

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

- The partner is an MSP with between \$3 million and \$5 million in annual revenue and 20 to 30 employees.
- It is headquartered in North America and serves clients globally in EMEA and APAC.
- It is partnered with ConnectWise and uses its solutions to operate a nonsecurity managed services offering.
- With the help of ConnectWise Cybersecurity Management, it adds a security component to its managed-services offering. This enhanced offering enables the composite to charge a premium for its managed services and better serve clients.
- Prior to enhancing its managed services offering with ConnectWise Cybersecurity Management, the composite partner had 100 customers. It charges for this service on a per-seat per-month basis.

Key Assumptions

- **North American MSP with global clients**
- **\$3 million to \$5 million annual revenue**
- **20 to 30 employees**
- **100 preexisting clients**
- **Existing nonsecurity managed services offering**
- **Enhances its managed services offering with ConnectWise Cybersecurity Management solutions**

Analysis Of Partner Revenue Streams

■ Quantified revenue data as applied to the composite

Revenue Streams And Gross Profits

Ref.	Revenue Streams	Year 1	Year 2	Year 3	Total	Present Value
At	Cybersecurity managed services annual gross profit	\$273,000	\$733,785	\$1,389,960	\$2,396,745	\$1,898,913
	Total gross profit	\$273,000	\$733,785	\$1,389,960	\$2,396,745	\$1,898,913

CYBERSECURITY MANAGED SERVICES ANNUAL GROSS PROFIT

Evidence and data. Interviewees told Forrester how they used ConnectWise Cybersecurity Management solutions to enhance their organizations' preexisting managed services offerings. Before using ConnectWise Cybersecurity Management solutions, the organizations used other ConnectWise solutions including Unified Monitoring & Management and Business Management to serve clients. But with Cybersecurity Management, interviewees stated that their organizations were able to deliver better services to existing clients, attract new clients, price their services higher, and achieve better gross margins with limited additional effort and resources.

- Interviewees said that after building their organizations' enhanced managed services offerings, they saw expansion rates of 10% to 35% per year as they expanded existing clients to their improved offerings at higher prices. The managing director of a European MSP for SMBs noted: "We're only 25% to 30% through. Next year, the target is to get over 80% on that pricing."
- A general manager of IT services for a North American MSP and general IT services organization said, "80% [of my firm's existing managed services clients] are [already] security customers."
- Besides expanding the offering to existing customers, interviewees also noted how the quality of their organizations' enhanced offerings and ConnectWise's Cybersecurity Management partner program fueled new customer growth. The managing director of a European MSP for SMBs with 96 customers noted, "We aim for seven new customers a year."
- The business owner of an Australian MSP explained how the ConnectWise partner program helped with new customer growth. They stated: "With this one client ... I'd say it weighed heavily on the client to move that quickly. ... [I'd attribute] maybe between 25% and 50% [to the partner program] pushing it over the line."

"I've already had the opportunity to take a couple of the senior [ConnectWise experts] into meetings with my clients... that's the real benefit, being able to engage those product experts at that level and put them in front of clients. That's led to closing deals. No question."

Business owner, Australian MSP

- Interviewees reported managing an average of up to 31 seats per customer.
- While interviewees reported a range of prices before using ConnectWise Cybersecurity Management solutions, they consistently reported significant price increases of 50% to 100% after enhancing their organizations' managed services offerings.
- The business owner of an Australian MSP discussed their firm's security-driven price increase: "Our average seat is between \$94 and \$105 [per] user. For the high compliance with output, [we charge] \$157 to \$175."
- The managing director of a European MSP for SMBs said, "[We] doubled [our pricing], and we are not getting any pushback."

“The primary driver [of our new package] is the 24/7 SOC, and that enabled us to take up our seat price from £40 per seat to £80 per seat.”

Managing director, European MSP for SMBs

- Interviewees indicated that compared to standard managed services, higher gross margins were possible with security managed services. The managing director of a European MSP for SMBs said, "Profit-wise, ... we've added five points." The general manager of IT services for a North American MSP and general IT services organization noted: "For managed services, we'll rate around 40%. [But, with ConnectWise Cybersecurity Management solutions, there's a] 60% margin and 85% of the work is done by ConnectWise."

Higher gross margin vs. other managed services for North American MSP and general IT services organization

1.5x

Modeling and assumptions. Forrester assumes:

- The composite partner has an existing managed services offering, and it enhances it with ConnectWise Cybersecurity Management solutions. This enables more value for clients and allows for higher pricing.
- The composite partner has 100 preexisting managed services customers, and it expands some of these customers to the new, higher price point each year. It also adds new customers.
- The composite partner has a high managed services retention rate.
- The average number of seats per customer increases over time as the composite partner's clients grow and consume more services.
- The composite partner's gross margin improves year-over-year from efficiency gains due to training and experience.

Risks. This revenue stream may vary based on:

- The number of preexisting clients and the rate at which the organization expands its new offering and pricing to them.
- The new customer growth rate.
- The organization's customer retention rate.
- The size of the organization's clients and the corresponding number of seats they purchase.

- The organization’s pricing before and after enhancing its managed services offering with ConnectWise Cybersecurity.
- The average managed services gross margin and the organization’s capability to improve and gain efficiency year-over-year.

Results. Forrester calculated a three-year total PV gross profit (discounted at 10%) of \$1.90 million.

“Our growth in security will be at least 50% this year, if not more. Our overall growth is 35%.”

General manager of IT services, North American MSP and general IT services organization

Cybersecurity Managed Services Annual Gross Profit					
Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Preexisting customer expansion rate with cybersecurity managed services	Interviews	25%	25%	25%
A2	Preexisting customers expanded to cybersecurity managed services	100*A1	25	25	25
A3	Organic new-customer growth rate	Interviews	7%	7%	7%
A4	ConnectWise Cybersecurity Management partnership and offering-attributed additional new customer growth rate	Interviews	3%	3%	3%
A5	Subtotal: ConnectWise Cybersecurity Management new-customer growth rate	A3+A4	10%	10%	10%
A6	New cybersecurity managed services customers per year	(100+A6^{PY})*A5	10	11	12
A7	Subtotal: Cumulative cybersecurity managed services customers	A2+A6+A7 ^{PY}	35	71	108
A8	Average number of seats per customer	Interviews	20	25	30
A9	Subtotal: Cumulative seats managed	A7*A8	700	1,775	3,240
A10	Price per seat per month before ConnectWise Cybersecurity Management	Interviews	\$100	\$100	\$100
A11	Price per seat increase with ConnectWise Cybersecurity Management	Interviews	65%	65%	65%
A12	Price per seat per month after ConnectWise Cybersecurity Management	A10*A11	\$165	\$165	\$165
A13	Subtotal: Cybersecurity managed services annual revenue	A9*(A12-A10)*12	\$546,000	\$1,384,500	\$2,527,200
A14	Average gross margin for security managed services	Interviews	50%	53%	55%
At	Cybersecurity managed services annual gross profit	A13*A14	\$273,000	\$733,785	\$1,389,960
Three-year total: \$2,396,745			Three-year present value: \$1,898,913		

UNQUANTIFIED BENEFITS

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

- **Superior client outcomes, including improved security posture and lowered risk.**

Interviewees said ConnectWise Cybersecurity Management solutions allowed their organizations to deliver better outcomes for their customers faster, improved their clients' security postures, and lowered their customers' risks of attacks with 24/7 coverage and faster response times. The managing director of a European MSP for SMBs noted, "The overall level of our audited risk has improved [for each customer]."

The CEO of a North American MSP for SMBs said: "The average response time for MSPs or internal IT teams is 14 hours to a ransomware attack. Our average response-time is under 14 minutes, and it's really less than 4 minutes from the initial response from the initial notification to win [with the SOC]. ... There's no way I could respond that quickly [without ConnectWise]."

"We can protect those [assets] in real time for clients with minimal staff by leveraging all this technology from ConnectWise and knowing that when there is an incident, we get a response from ConnectWise as though we were a Fortune 500 [company] ourselves. ... It's impressive to the client."

CEO, North American MSP for SMBs

"The security partnership has been a huge boost to business. It's enabled us to offer 24/7 SOC services and reassurance to our clients without any huge investment. We can remove the need for our clients to look elsewhere for their services, and we de-risked our client base. We've leveraged that extra capability to increase our pricing quite significantly, and that's worked out well."

Managing director, European MSP for SMBs

- **Improved, scaled, automated, and focused operations.** Besides helping their organizations' clients succeed, interviewees discussed how partnering with ConnectWise helped improve their firms' own internal operations. Interviewees spoke of the improved service availability, automation and scalability, incident reduction, and more.

The CEO of a North American MSP for SMBs explained: "In the IT environment when we first started this business, all we did all day long was put out fires and keep businesses functional and optimized as much as possible. It was really break-fix running around putting out fires all day long. [But with ConnectWise Cybersecurity Management solutions,] we were able to eliminate over 95% of all the noise simply by putting the right tools in place to allow businesses to just function."

Additionally, the business owner of an Australian MSP said that ConnectWise’s 24/7 SOC and improvements to the firm’s operations allowed their team to devote time to value-add activities. They said: “It’s always senior engineers that get pulled into those kinds of situations. My highest-value engineers got tied up for hours. That’s where the cost benefit is. If I can free up those engineers to be doing billable hours on other more proactive work or projects or revenue-creating tasks, then that’s where my margin is.”

- **Significant 24/7 SOC savings.** Interviewees highlighted how their organizations could enjoy using an SOC without the cost of running one themselves. To run an SOC, interviewees estimated their organizations would have to hire six to 20 FTEs. The business owner of an Australian MSP stated, “It’s unfeasible for a small MSP to even consider doing that.” The CEO of a North American MSP and general IT services organization said, “You’re looking at well over a million dollars in resources to create what we get for a fraction of that cost from ConnectWise.”
- **Cyber insurance support and benefits.** Interviewees said that with ConnectWise Cybersecurity Management solutions, their organizations could help clients prepare for cyber insurance, which could later reimburse for services. The general manager of IT services of a North American MSP and general IT services organization said: “ConnectWise allows us to prepare customers for cybersecurity insurance. ... which is a project for us. ConnectWise has helped us with that template and with the tools to implement that.”
- **Support, collaboration, and relationships.** Last, the interviewees detailed how they welcomed working with ConnectWise, valued the support their organizations received, and appreciated being a part of the greater community both online and in person at events.

“One of the big values [ConnectWise] has on the security side is [that it’s] a partner. ... Whenever we’re researching or looking to do something, we have one person within ConnectWise we can go to. Then behind them is a set of experts [including] high-level people.”

General manager of IT services, North American MSP and general IT services organization

FLEXIBILITY

The value of flexibility is unique to each partner. There are multiple scenarios in which a ConnectWise Cybersecurity Management partner might implement a Cybersecurity Management practice and later realize additional opportunities, including:

- **Follow-on security professional services.** Interviewees said that by enhancing their organizations’ managed services offerings with ConnectWise Cybersecurity Management solutions, they had the opportunities to offer additional types of security services. In particular, interviewees noted that when a client suffered a breach, their organizations could now conduct remediation work with ConnectWise’s SOC team and the client’s cyber insurance would cover it. They also gained the ability to offer different pricing structures, like for a breach-hours retainer.

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

Analysis Of Partner Investments

■ Quantified investment data as applied to the composite

Total Investments							
Ref.	Investments	Initial	Year 1	Year 2	Year 3	Total	Present Value
Bt	Cybersecurity managed services practice investments	\$19,110	\$57,330	\$145,373	\$265,356	\$487,169	\$390,737
	Total investments	\$19,110	\$57,330	\$145,373	\$265,356	\$487,169	\$390,737

CYBERSECURITY MANAGED SERVICES PRACTICE INVESTMENTS

Evidence and data. Beyond the cost of ConnectWise Cybersecurity Management solutions and other delivery costs, interviewees discussed other operating expenses included:

- **Research and development investments.** With the enhancement of their organizations’ managed services offerings, interviewees stated there was a need for initial practice setup and research and ongoing research. Some interviewees’ organizations even had dedicated security experts on staff who could devote time to research and bettering their practices.
- **Training investments.** Interviewees said that as their organizations were building their new security practices, it was important to train their delivery and sales staff on ConnectWise Cybersecurity Management solutions and their enhanced managed service offerings.

The managing director of a European MSP for SMBs said, “[To learn how to sell security,] we’ve had on the sales side six or eight days of sales training [for many employees].” The general manager of IT services of a North American MSP and general IT services organization said: “ConnectWise does have ConnectWise University that has training and certifications. I

would say we spend 8 hours a quarter [on training].” The business owner of an Australian MSP said, “Training is becoming more and more important.”

- **Sales and marketing investments.** Interviewees discussed their organizations’ marketing strategies, including in-person events and the marketing support and funding they receive from ConnectWise. The general manager of IT services for a North American MSP and IT services organization said: “All our marketing campaigns for next year are focused on security solutions. ... We did not have any proactive consulting around risk assessments or penetration tests, and we [now] leverage ConnectWise to help us with that.”
- **General and administrative investments.** Interviewees said these investments included office spaces, utilities, and other back-office functions such as billing, finance, accounting, and legal. The managing director of a European MSP for SMBs broke down their organization’s roles including finance. They said: “We have two [employees] in finance, one in marketing, four in sales, three in technical alignment, [and] four in professional services, and the rest are on service desk or service delivery for managed agreements. One [is also] in security and one [is] in [the] NOC (network operations center).”

Modeling and assumptions. Forrester assumes:

- Beyond service delivery costs, the composite partner invests a percentage of practice revenue for operations.
- Research and development investments represent 1% of practice revenue, including an initial investment (inferred from Year 1).
- Training investments represent 2.5% of practice revenue, including an initial investment (inferred from Year 1).

- Sales and marketing investments represent 5% of practice revenue.
- General and administrative investments represent 2% of practice revenue.

Risks. This investment may vary based on the organization’s unique investment requirements, decisions, operations, and costs.

Results. Forrester calculated a three-year total PV investment (discounted at 10%) of \$391,000.

Cybersecurity Managed Services Practice Investments						
Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
B1	Total cybersecurity managed services practice revenue	A13	\$0	\$546,000	\$1,384,500	\$2,527,200
B2	Research and development investments	B1*1%	\$5,460	\$5,460	\$13,845	\$25,272
B3	Training investments	B1*2.5%	\$13,650	\$13,650	\$34,613	\$63,180
B4	Sales and marketing investments	B1*5%	\$0	\$27,300	\$69,225	\$126,360
B5	General and administrative investments	B1*2%	\$0	\$10,920	\$27,690	\$50,544
Bt	Cybersecurity managed services practice investments	B2+B3+B4+B5	\$19,110	\$57,330	\$145,373	\$265,356
Three-year total: \$487,169			Three-year present value: \$390,737			

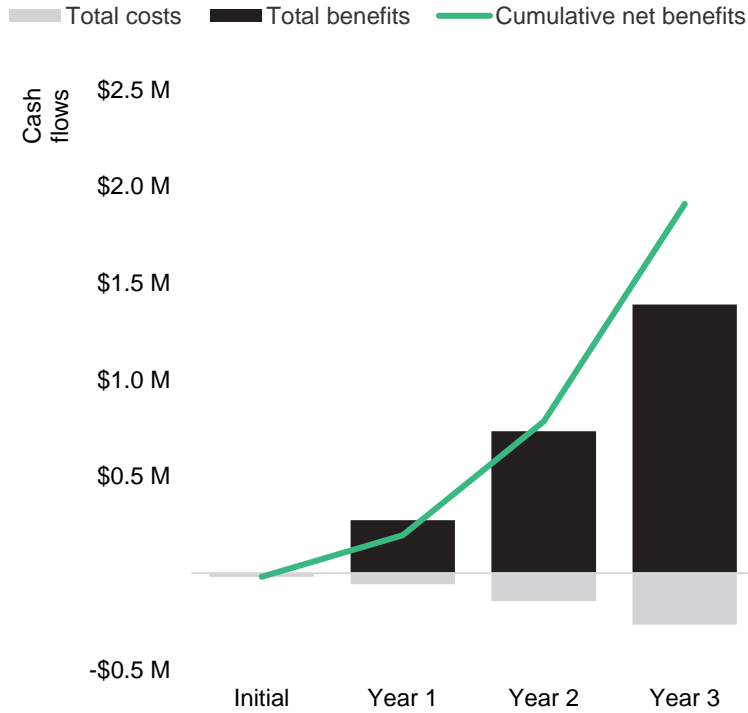
“Our investment in ConnectWise has been incredibly positive. It’s been a great partnership. The support we get from them ... has been the best I have ever received, and the most easily accessible.”

— Managing director, European MSP for SMBs

Financial Summary

CONSOLIDATED THREE-YEAR METRICS

Cash Flow Chart



The financial results calculated in the Revenue Streams and Investments 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 ROI, NPV, and payback period values are determined from the results in each Revenue Stream and Investment section.

Cash Flow Analysis

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	(\$19,110)	(\$57,330)	(\$145,373)	(\$265,356)	(\$487,169)	(\$390,737)
Total benefits	\$0	\$273,000	\$733,785	\$1,389,960	\$2,396,745	\$1,898,913
Net benefits	(\$19,110)	\$215,670	\$588,412	\$1,124,604	\$1,909,576	\$1,508,176
ROI						386%

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: “Planning Guide 2023: Security & Risk,” Forrester Research, Inc., August 23, 2022.

² Total Economic Impact is a methodology developed by Forrester Research that enhances a company’s technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

FORRESTER®