FORRESTER®

The Total Economic Impact™ Of BlueVoyant Managed Detection And Response (MDR) Services

Cost Savings And Business Benefits Enabled By BlueVoyant MDR Services

A FORRESTER TOTAL ECONOMIC IMPACT STUDY
COMMISSIONED BY BLUEVOYANT, JULY 2024

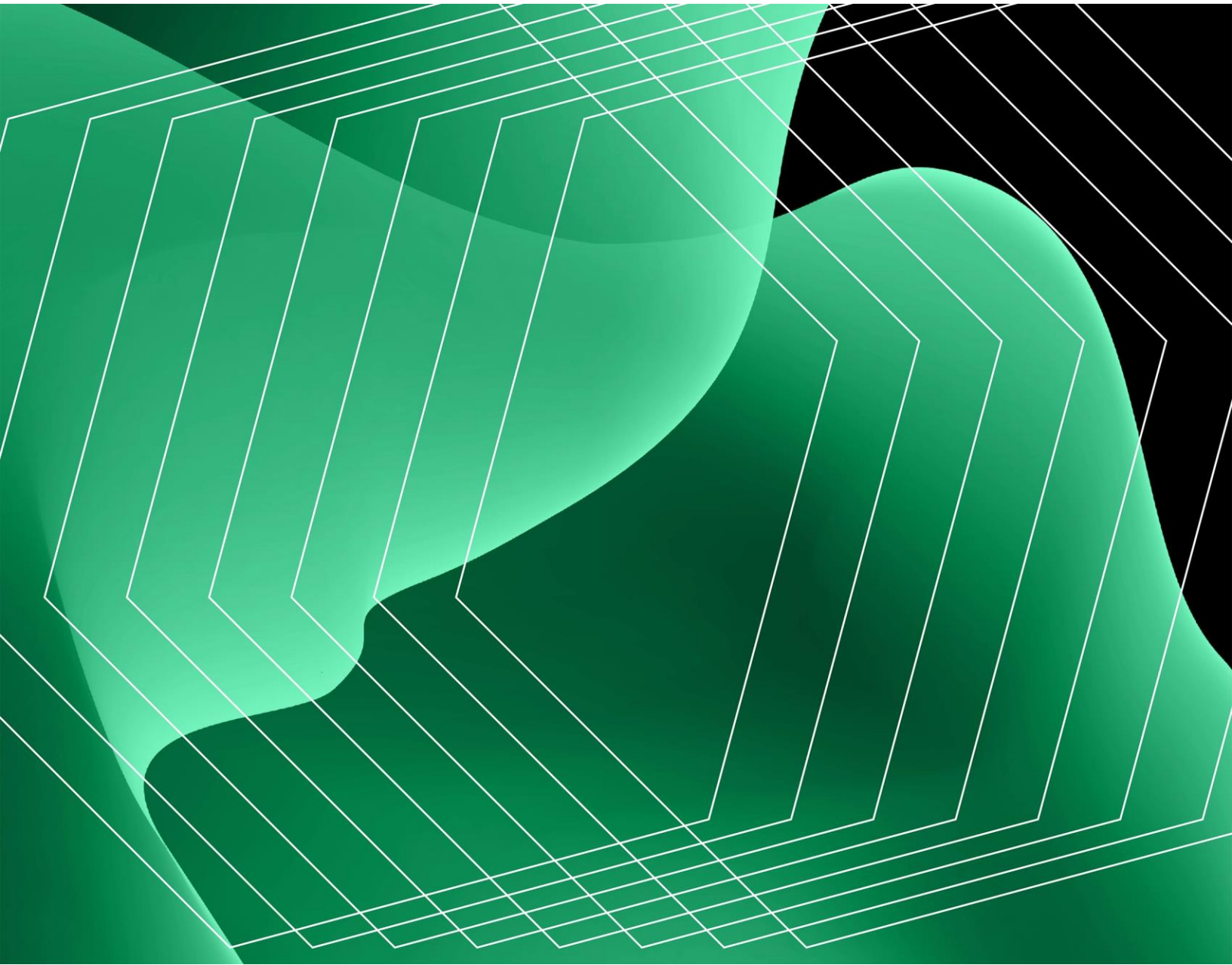


Table Of Contents

Consulting Team:

Nikoletta Stergiou

ABOUT FORRESTER CONSULTING

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

Executive Summary

In an increasingly hostile threat landscape, organizations with a lack of resources and overworked security operations teams cannot provide effective, full-coverage threat detection and response. BlueVoyant MDR services enables organizations with a cloud-native solution that offers end-to-end consulting, implementation, and managed security services with 24/7 security threat detection and response.

Analysts from BlueVoyant offer military-grade expertise with deep experience in cyber defense. BlueVoyant enables customers to better automate their alerts to reduce fatigue and have full visibility into incidents, assets, vulnerabilities, and ongoing investigations to strengthen their organization's overall security posture.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using MDR services. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a global organization with $5 billion in annual revenue, 10,000 employees, and 15,000 endpoints.

Return on investment (ROI)
210%

Net present value
$3.88M

Interviewees said that prior to using BlueVoyant's MDR services, their organizations utilized multiple point solutions, internal labor to manage their security operations, and external security operations center (SOC) teams. However, prior attempts yielded limited success, leaving them with ineffective SOC coverage, complex implementation and data migration processes with legacy solutions, excess security information and

event management (SIEM) spending, and a lack of visibility into the organization's security environment. These limitations led to false and excess security alerts which fatigued security operations, and left their organizations vulnerable to potential attacks. Their prior solutions also provided a lack of scalability and integrations.

After the investment in BlueVoyant's MDR services, the interviewees noted that BlueVoyant's advanced automation and expert SOC analyst support enabled them to free up and reallocate internal security resources, driving an improvement in their organization's overall security posture and visibility. Key results from the investment include labor cost savings from reduced alerts, optimized spending, and avoided costs for breaches.

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Labor cost savings from reduced total escalated alerts per month by 90% with BlueVoyant.** BlueVoyant's technology and processes help security operations (SecOps) teams reduce the number of alerts that need to be addressed manually as well as a faster mean time to resolution (MTTR). By leveraging automation and advanced threat intelligence capabilities, BlueVoyant can filter out false positives and identify non-malicious incidents, which enables SecOps analysts to reallocate time toward other value-added activities such as cyber threat hunting. Over three years, labor cost savings from reduced alerts is worth more than $907,000 to the composite organization.
- **Optimized spending by more than $895,000.** BlueVoyant enables the composite organization to optimize spending by consolidating legacy tools. This improves efficiency as the SecOps team can focus on a single platform, which saves time and effort on administration. It enables better data integration and correlation, enhancing visibility and informed decision-making as a comprehensive solution. Spending is further optimized by avoiding the need for

> “BlueVoyant has been a trusted partner to myself, to my boss, and to the senior leaders that run our 24/7 SOC. I’ve appreciated all of their insights, and most importantly, their brutal honesty on our existing operations. Sometimes you need a third party to tell you what you’re doing right, but more importantly, to tell you what you’re doing wrong so that you can reduce the risk within the enterprise.”
>
> **DEPUTY ENTERPRISE CISO, INSURANCE**

1.5 security engineer FTEs to support legacy solutions, worth more than $895,000 over three years.

- **Avoided breach costs by more than $3.9 million.** On average, the composite organization is exposed to 2.5 major breaches annually, with the potential to impact more than 2,000 endpoints. The cost of a single security breach is approximately $756,500 for the composite, on top of $810,000 worth in downtime from impacted business end users. BlueVoyant improves the security posture for the composite organization through expert analysis and response capabilities that provide employees with actionable insights to ultimately reduce the likelihood of a breach. Over three years, this cost avoidance is worth more than $3.9 million.

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified for this study include:

- **Faster SIEM onboarding.** BlueVoyant streamlines the onboarding process for the composite organization’s SIEM solution to be as efficient as possible. Most employees were able to onboard within a couple of months, with various steps including scoping, deployment, integration, and configuration.
- **Improved visibility and insights.** BlueVoyant’s solutions provides the composite organization with a holistic view of its security posture, enabling employees to understand the evolving threat landscape, detect potential risks,

and make informed decisions. BlueVoyant's expertise and partnership optimizes the composite organization's security operations by enhancing its employees' understanding of their security landscape.

- **Improved employee experience (EX).** Adding BlueVoyant to security operations improves the composite organization's overall EX by making workloads more manageable.
- **Partnership with BlueVoyant.** Having BlueVoyant as a partner offers benefits that enable employees to continuously learn from their expertise and insights as an industry leader.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **BlueVoyant licensing fees.** BlueVoyant's licensing is a subscription fee based on endpoint count. Prior to using BlueVoyant, some licensing costs for legacy tools validated a volume-based licensing approach for a significant number of endpoints.
- **Implementation and training costs.** The implementation process for BlueVoyant is a collaboration between the security team and the BlueVoyant team. It typically takes two months to completely onboard the SIEM solutions.
- **Ongoing management costs.** Ongoing management involves regular check-ins, reporting, and collaboration with the BlueVoyant team.

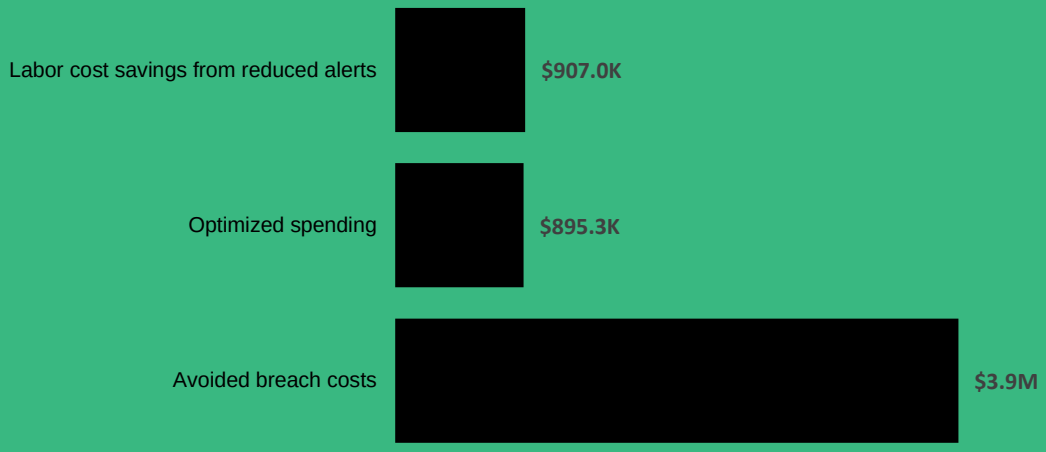
The representative interviews and financial analysis found that a composite organization experiences benefits of $5.73 million over three years versus costs of $1.85 million, adding up to a net present value (NPV) of $3.88 million and an ROI of 210%.

Reduction in total escalated alerts per month with BlueVoyant:

90%

ROI	BENEFITS PV	NPV	PAYBACK
210%	**$5.73M**	**$3.88M**	**<6 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 BlueVoyant's MDR services.

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 BlueVoyant's MDR services can have on an organization.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by BlueVoyant 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 BlueVoyant's MDR services.

BlueVoyant 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.

BlueVoyant provided the customer names for the interviews but did not participate in the interviews.

1. **Due Diligence**
   Interviewed BlueVoyant stakeholders and Forrester analysts to gather data relative to BlueVoyant's MDR services.
2. **Interviews**
   Interviewed four representatives at organizations using BlueVoyant's MDR services to obtain data about costs, benefits, and risks.
3. **Composite Organization**
   Designed a composite organization based on characteristics of the interviewees' organizations.
4. **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.
5. **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 BlueVoyant MDR Services Customer Journey

Drivers leading to the MDR services investment

Interviews					
Role	**Industry**	**Region**	**Average Annual Revenue**	**Number of Employees**	**Endpoints**
Director of cyber defense	Retail	Headquartered in the US, global operations	$2.6 billion	14,400	10,000
Deputy enterprise CISO	Insurance	Headquartered in the US, global operations	$14.3 billion	13,500	10,500
CISO	Manufacturing	Headquartered in the US	$4 billion	5,000	22,500
CSO	Healthcare	Headquartered in the US, global operations	$9 billion	35,000	35,000

KEY CHALLENGES

Before implementing BlueVoyant's MDR services, the interviewees' organizations faced significant challenges in their security posture from a range of legacy point solutions. They experienced a lack of effective SOC coverage, complex implementation and data migration with legacy solutions, excess spending on SIEM technology, and the lack of visibility into the security environment, that left them vulnerable to an increased the risk of data breaches and other security incidents.

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

- **Lack of effective SOC coverage.** Interviewees noted the risk of security breaches and incidents due to a lack of effective 24/7 SOC coverage. This issue often stemmed from the expensive investment required to establish and maintain round-the-clock security operations, as well as the lack of available talent in the

cybersecurity field. Without constant monitoring and response, interviewees noted that they might miss critical security events that could expose them to potential attacks.

The CSO at a healthcare organization described the limited SOC functionalities in their prior state: “The threat hunting and SOC was all being handled by a limited number of analysts and security engineers who were depending on [assigning someone to look at an alert if it came in]. There wasn’t a defined role for the cyber threat analyst inside the organization at the time.”

The director of cyber defense at a retail organization described implementation challenges with their previous point solution: “Implementation [for our previous point solution] was not going well when I came on, and we struggled with it going forward. We found that it was very difficult to bring information and integration with our cloud native workloads. We were not getting a lot of integration and correlation with log sources out of it.”

- **Excess SIEM spending.** Interviewees noted heavy investments in prior SIEM technology which resulted in high costs and excess alerts. Inflated costs, a lack of necessary expertise to effectively manage and configure the SIEM solution, and the potential underutilization of the solution's capabilities caused the interviewees organizations to potentially miss security threats and resulted in inefficient operations.

  The deputy CISO at an insurance organization commented, “We had a third-party provider who we were spending millions on and we were generating a lot of alerts.”

- **Lack of visibility into security environment.** Interviewees highlighted that without proper insight into the devices and systems connected to a network, their organizations struggled to always detect and respond to potential threats. This lack of visibility left blind spots that could be exploited by attackers, potentially leading to data breaches or other security incidents.

  The deputy enterprise CISO at an insurance organization described the lack of visibility in their prior environment: “The solutions we had were essentially engineered for each operating company. Monitoring these assets became problematic. I think that the vulnerability was the fact that we needed to have a more complete picture of our landscape for our environment across all the

different operating companies so that if there was a cyberattack, we'd be able to quickly identify it and contain it."

- **False and excess security alerts.** Interviewees noted that false and excess security alerts overwhelmed security teams and led to alert fatigue. A high volume of alerts made it challenging to differentiate genuine threats from false positives, causing security teams to waste time and resources investigating non-existent or low-risk issues.

  The deputy enterprise CISO at an insurance organization described the impact of high costs related to the investigation of false positives: "Our previous third-party provider was happy to process all the different alerts from the phishing inbox that was being sent their way. If we hadn't transitioned to BlueVoyant, we would have continued paying that money without most people thinking about it."

- **Lack of scalability and integration.** Interviewees noted that while their organizations grew and evolved, their security must change as well. Prior security solutions limited the scalability and integration of other systems, which became inadequate for the requirements of the interviewees' organizations. This left vulnerabilities unaddressed and hindered their organizations' overall security postures.

  The director of cyber defense at a retail organization commented: "BlueVoyant plugs together very nicely and we kind of knew that going in. So when we turned the switch to enable [a cloud-native solution] on that log analytics workspace, it was basically checkboxes through much of the interface. All of the things that we were fighting with API integrations on [our prior point solution] were just checkboxes to get in."

- **Complex implementation and data migration with legacy solutions.** Interviewees highlighted that the process of integrating legacy solutions into existing systems and migrating data was time-consuming and prone to errors. This complexity led to delays in implementing necessary security measures and hindered organizations from effectively leveraging their security investments.

INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Reallocate security resources.
- Improve managed detection and response (MDR) and security posture.
- Improve endpoint visibility.
- Improve efficiency through automated processes.
- Centralize and consolidate solutions.
- Reduce cloud consumption costs.

> “Prior to BlueVoyant, it was pure staff burnout. When you have some of your security engineers and analysts now working 16-hour days, that quickly leads to turnover.”
>
> **CSO, HEALTHCARE**

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite 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:

Description of composite and deployment characteristics. The global organization has $5 billion in annual revenue, 10,000 employees, and 15,000 endpoints. The SecOps team consists of 10 FTEs.

KEY ASSUMPTIONS

$5 billion annual revenue

10,000 employees

15,000 endpoints

10 SecOps FTEs

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	Labor cost savings from reduced alerts	$364,721	$364,721	$364,721	$1,094,164	$907,008
Btr	Optimized spending	$360,000	$360,000	$360,000	$1,080,000	$895,267
Ctr	Avoided breach costs	$1,580,167	$1,580,167	$1,580,167	$4,740,501	$3,929,641
	Total benefits (risk-adjusted)	$2,304,888	$2,304,888	$2,304,888	$6,914,665	$5,731,916

LABOR COST SAVINGS FROM REDUCED ALERTS

Evidence and data. BlueVoyant's technology and processes reduces the number of alerts that need to be addressed by the analysts at the interviewees' organizations. By leveraging automation and advanced threat intelligence capabilities, BlueVoyant filters out false positives and identifies non-malicious incidents. This allowed interviewees' security teams to focus their time and efforts on addressing genuine threats rather than wasting resources on investigating and responding to false alarms. The interviewees' security teams could then work more efficiently and effectively, maximizing their impact and reducing the financial burden of unnecessary alert processing.

- The CSO at a healthcare organization discussed the impact that reduced MTTR with BlueVoyant had on reallocating talent to other critical activities including cyberthreat hunting, "Part of that is the force multiplier that we get out of BlueVoyant, and soon after we signed the contract with them I was able to move one of my security analysts over to be a full-time cyber threat hunter. Since then, I have been able to hire two more threat analysts."
- The director of cyber defense at a retail organization noted the impact of reduced false positive alerts and improved MTTR: "It's very rare that we have an escalation that is a false positive from BlueVoyant. We've also reduced MTTR, and a lot of that comes from the alerts that are being closed with BlueVoyant

because they don't need to be escalated. BlueVoyant is handling that and that is back to their automations and their internal practices that really gets us ahead."

- The deputy enterprise CISO at an insurance organization discussed the cost savings from automated resolution with BlueVoyant: "BlueVoyant did an analysis and found about 90% of the things that were reported were not malicious. That has a real-world impact because it cost us millions of dollars that we were spending for our third party, who was happy enough to take those alerts and process them."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Prior to BlueVoyant, 4,000 alerts were escalated on a monthly basis, of which, 40% were manually resolved by the SecOps team. On average, it took 20 minutes to resolve these alerts without BlueVoyant.
- With BlueVoyant, the total number of escalated alerts is reduced by 99% and MTTR is reduced by 70%.
- The average hourly fully-burdened rate of a SecOps FTE is $68.50.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Number of alerts escalated to be manually resolved in an organization.
- Average MTTR for alerts.
- Average hourly fully-burdened rate of a SecOps FTE.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $907,000.

Reduction in total escalated alerts per month with BlueVoyant

99%

> "In the past, mean time to close was in a few hours' time. With BlueVoyant, the average is probably faster by 70% to 80%."
>
> CISO, MANUFACTURING

Labor Cost Savings From Reduced Alerts					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Escalated alerts in prior environment (monthly)	Composite	4,000	4,000	4,000
A2	Percentage of escalated alerts manually resolved by SecOps team in prior environment	Composite	40%	40%	40%
A3	Alerts manually resolved by SecOps team in prior environment (monthly)	A1*A2	1,600	1,600	1,600
A4	Percentage reduction in total escalated alerts per month with BlueVoyant	Interviews	90%	90%	90%
A5	Alerts manually resolved by SecOps team with BlueVoyant (monthly)	A1*(1-A4)	400	400	400
A6	Alerts eliminated by BlueVoyant for the SecOps team (monthly)	A3-A5	1,200	1,200	1,200
A7	Average MTTR (minutes)	Composite	20	20	20
A8	**Subtotal: Hours saved from eliminating alerts with BV (monthly)**	**(A6*A7)/60 minutes**	**400**	**400**	**400**
A9	Improvement in MTTR for alerts with BlueVoyant	Interviews	70%	70%	70%
A10	**Subtotal: Hours saved from reduced MTTR with BlueVoyant (monthly)**	**(A5*A7*A9)/60 minutes**	**93**	**93**	**93**
A11	Average hourly fully-burdened salary of a SecOps FTE	Composite	$68.50	$68.50	$68.50
At	Labor cost savings from reduced alerts	(A8+A10)*A11*12 months	$405,246	$405,246	$405,246
	Risk adjustment	↓10%			
Atr	Labor cost savings from reduced alerts (risk-adjusted)		$364,721	$364,721	$364,721
Three-year total: $1,094,164			**Three-year present value: $907,008**		

OPTIMIZED SPENDING

Evidence and data. Interviewees highlighted that BlueVoyant helped them optimize spending as the solution offers a centralized platform that integrates various cybersecurity solutions, eliminating the need for multiple standalone tools. Consolidating tools helped interviewees improve efficiency as security teams could focus on a single platform, saving time and effort on administration. It also enabled better data integration and correlation, enhancing visibility and informed decision-making. Overall, BlueVoyant's tool consolidation simplified the security infrastructure, reduced costs, and improved the effectiveness of cybersecurity operations for the interviewees' organizations.

- The CISO at a manufacturing organization discussed the impact of centralizing their tools with BlueVoyant: "With BlueVoyant, we're able to bridge different technologies and help us manage the alerts from different tools, which in certain cases have a lot of overlap. BlueVoyant helped to create automation and alerts, which helped us fine-tune what we truly needed to focus on."
- The director of cyber defense at a retail company discussed breaking a contract with their prior [network security management platform]: "We were on a three-year term with our [previous network security management platform]. It was about a year and a half into it when we decided to make the transition to BlueVoyant and the cost savings by going to the shared MDR service from the fully-outsourced SOC allowed me to recognize the [legacy tool] as a sunk cost."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Adopting BlueVoyant retires $175,000 in licensing costs for legacy solutions.
- Avoids the need for 1.5 security engineer FTEs to support legacy solutions.
- The average annual fully-burdened salary of a security engineer is $150,000.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Licensing costs related to retired legacy solutions.
- Number of security engineer FTEs needed to support legacy solutions.

- The average annual fully-burdened salary of a security engineer.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $895,000.

Avoided security engineer FTEs needed to support legacy solutions

1.5

Optimized Spending					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Retired legacy solutions licensing costs	Interviews	$175,000	$175,000	$175,000
B2	Security engineer FTEs needed to support legacy solution	Interviews	1.5	1.5	1.5
B3	Average annual fully-burdened salary of a security engineer	Composite	$150,000	$150,000	$150,000
Bt	Optimized spending	C1+(C2*C3)	$400,000	$400,000	$400,000
	Risk adjustment	↓10%			
Btr	Optimized spending (risk-adjusted)		$360,000	$360,000	$360,000
	Three-year total: $1,080,000			**Three-year present value: $895,267**	

“Our [prior network security management platform] and SOAR [security orchestration, automation, and response] platform were decommissioned as a result of our investment in BlueVoyant.”

CISO, MANUFACTURING

AVOIDED BREACH COSTS

Evidence and data. Interviewees discussed how BlueVoyant improved the security posture of their organization, which ultimately reduced the likelihood of breaches. BlueVoyant's expertise and analysis provided actionable insights to interviewees to understand the evolving threat landscape and make informed security decisions in their environment. They assisted interviewees in identifying and remedying vulnerabilities through comprehensive assessments and penetration testing, which validated BlueVoyant's capabilities and justified the interviewees' investment in the solution.

- The CISO at a manufacturing organization described a red team exercise BlueVoyant quickly detected and acted on: "There was a critical event created by an external red team we hired. I think that the engagement was within a minute. Once BlueVoyant caught them within a minute, everybody was on a triage call and the investigation took another few minutes. We didn't share that it's an external red team, so BlueVoyant just implemented some defensive tactics and blocked them."
- The deputy enterprise CISO at an insurance organization highlighted BlueVoyant's intervention on a potential ransomware incident: "We've had phishing instances since BlueVoyant has been around, in which an employee clicked on a [phishing attempt] and there was malware that was loaded onto his laptop, we were able to get an alert based on it and it was the early stages of a potential ransomware incident. That is probably the primary threat vector that I care about all the time."
- The director of cyber defense at a retail organization discussed BlueVoyant's successful detection of penetration tests: "I run annual penetration tests and BlueVoyant never knows when I'm going to do it. They have been able to alert us to everything that we've had in penetration tests. We've had great visibility and findings there which helps with control and validation."
- The CSO at a healthcare organization described a potential threat found by BlueVoyant on the dark web: "I think one of the things people may not be aware of is that BlueVoyant searches the dark web. They saw our name at one point and helped us track down something that was tied back to a vendor who was looking to sell our data on the dark web, which from that, we were able to move

very quickly and it led to the individual's arrest. This insight allowed my team to quickly respond and identify the actor and then reach out to law enforcement and get them involved."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The average cost of a security breach is $756,593. The cumulative cost of breaches includes average remediation and reporting labor costs, average costs of response and notification, fines, damages, compliance costs, customer compensation, average lost business revenues and additional costs to acquire customers, and end-user downtime as it relates to a security breach across the organization.
- There is an average of 2.5 major breaches per year. The percentage of endpoints impacted by each security breach is 15%. On average, there is 3.6 hours of downtime experienced with each breach.[2]
- With BlueVoyant, the likelihood of a data breach and its associated costs is reduced by 50%.
- The average fully-burdened hourly rate of a general business employee is $40.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Average number of major breaches experienced per year.
- Cost of a data breach for an organization.
- Total number of endpoints and percentage impacted by a breach.
- Average downtime hours experienced during each breach.
- Average fully-burdened hourly rate of a general business employee.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $3.93 million.

Reduction in likelihood of a data breach and its associated costs with BlueVoyant

50%

"BlueVoyant provides a level of assurance in our security posture. Every single corporation in America with this size and scale and the regulatory agents care about avoiding ransomware."

DEPUTY ENTERPRISE CISO, INSURANCE

Avoided Breach Costs

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Average number of major breaches annually	Forrester Research	2.5	2.5	2.5
C2	Cost per data breach	Forrester Consulting	$756,593	$756,593	$756,593
C3	Reduction in likelihood of a data breach and its associated costs with BlueVoyant	Forrester internal research	50%	50%	50%
C4	**Subtotal: Risk reduction savings due to BlueVoyant**	**C1*C2*C3**	**$945,741**	**$945,741**	**$945,741**
C5	Total business user endpoints	Composite	15,000	15,000	15,000
C6	Percentage of business user endpoints impacted by each breach	Forrester internal research	15%	15%	15%
C7	Average number of general business employee downtime hours per breach	Forrester Consulting	3.6	3.6	3.6
C8	Average fully-burdened hourly salary of a general business employee	Forrester Standard	$40	$40	$40
C9	**Subtotal: Cost to internal users for downtime and lost productivity**	**C1*C5*C7*C6*C8**	**$810,000**	**$810,000**	**$810,000**
Ct	Avoided breach costs	C4+C9	$1,755,741	$1,755,741	$1,755,741

	Risk adjustment	↓10%			
Ctr	Avoided breach costs (risk-adjusted)		$1,580,167	$1,580,167	$1,580,167
	Three-year total: $4,740,501		**Three-year present value: $3,929,641**		

UNQUANTIFIED BENEFITS

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

- **Faster SIEM onboarding.** Interviewees highlighted how BlueVoyant aimed to make the onboarding process for their SIEM solution as efficient as possible. Most interviewees were able to onboard within a couple of months, with various steps including scoping, deployment, integration, and configuration. BlueVoyant's experienced team ensured a smooth transition and minimal disruption to operations during the onboarding process.
- **Improved visibility and insights.** BlueVoyant's solutions provided the interviewees with a holistic view of their organization's security posture, enabling them to understand the evolving threat landscape, detect potential risks, and make informed decisions. BlueVoyant's expertise and partnership enhanced the composite organization's understanding of its security landscape and how to best optimize their security operations.

  The deputy enterprise CISO at an insurance organization commented: "The BlueVoyant team and their executive management provide us with strategic advice. They provide us with insights we don't have. What BlueVoyant does is it works with multinational corporations. There are insights to be gathered."
- **Improved EX.** Interviewees highlighted the impact that adding BlueVoyant to their organization's security operations had on overall EX. Prior to BlueVoyant, employees were overworked, and organizations faced turnover. With BlueVoyant, the workload became more manageable.

  The CSO at a healthcare organization commented: "One of the biggest things impacted was morale and retention. So, having that additional service that BlueVoyant provides has definitely assisted there."

- **Partnership with Bluevoyant.** Interviewees discussed the benefits of having BlueVoyant as a partner and continuously learning from their expertise and insights. The CISO at a manufacturing organization commented: “BlueVoyant has the ability to open a bridge and share their experiences with certain attacks, for example, if something happens and we read it on the news and just need additional feedback on how to improve our posture overall. They don’t even charge for this type of service because they don’t look at it as services. It’s just a matter of partnership.”

Average duration to onboard a SIEM solution with BlueVoyant

60 days

“With BlueVoyant, we had the unique opportunity to get a new SIEM, build it from scratch, find the gaps, have a new partner that could help us along the way, and have a partner that would be willing to go above and beyond to help us out.”

DEPUTY ENTERPRISE CISO, INSURANCE

> "We started with BlueVoyant fairly quickly because we did a proof of concept and during the proof of concept, we had already onboarded some of the key systems. That was something like a three-week process, and then I think within 60 days, we had almost everything transitioned."
>
> CISO, MANUFACTURING

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement BlueVoyant's MDR services and later realize additional uses and business opportunities, including:

- **Artificial intelligence (AI).** Some interviewees highlighted the potential impact that AI can have on their organization's overall security posture. The deputy enterprise CISO at an insurance organization discussed the potential impact that may come down the line as BlueVoyant's partnership further invests in security AI: "It also helps that BlueVoyant's partnership investment in AI early on and some of the cool new functionality that's embedded within their [security AI tool] will be an area in which we can further optimize our spending, perhaps reduce the number of full-time headcount and be able to outsource more functions to a provider like BlueVoyant."

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**
Dtr	BlueVoyant licensing fees	$0	$708,750	$708,750	$708,750	$2,126,250	$1,762,556
Etr	Implementation and training costs	$75,856	$0	$0	$0	$75,856	$75,856
Ftr	Ongoing management costs	$0	$5,425	$5,425	$5,425	$16,276	$13,492
	Total costs (risk-adjusted)	$75,856	$714,175	$714,175	$714,175	$2,218,382	$1,851,904

BLUEVOYANT LICENSING FEES

Evidence and data. BlueVoyant licensing is a subscription fee based on the number of endpoints. Some interviewees shared licensing costs which validated a volume-based licensing approach for organizations with a significant number of endpoints.

Licensing costs include subscriptions for Managed Azure Sentinel and Managed M365 Security, using a client-supplied Azure Sentinel subscription, correlated and analyzed network logs in real time, aggregated disparate data and the latest threat intelligence to filter background noise and identify real security concerns. This price is also inclusive of 20 hours of BlueVoyant Concierge Services.

- Pricing may vary. Contact BlueVoyant for additional details.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Annual licensing fees amount to $675,000.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Number of endpoints being managed by BlueVoyant.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.76 million.

BlueVoyant Licensing Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	BlueVoyant annual licensing fees	Composite		$675,000	$675,000	$675,000
Dt	BlueVoyant licensing fees	D1		$675,000	$675,000	$675,000
	Risk adjustment	↑5%				
Dtr			$0	$708,750	$708,750	$708,750
	Three-year total: $2,126,250		**Three-year present value: $1,762,556**			

IMPLEMENTATION AND TRAINING COSTS

Evidence and data. Interviewees described the implementation process for BlueVoyant as a collaboration between the security team and the BlueVoyant team. It typically took two months to completely onboard the interviewees' organizations SIEM solutions, with regular meetings and coordination to ensure a smooth transition. During this process, access provisioning and change were key steps. Training for employees focused on familiarizing them with the organization's specific tooling and procedures, with BlueVoyant's platform requiring minimal additional training.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- A BlueVoyant deployment services fee of $50,000, which includes an assessment of the client's pre-existing program, recommendations to improve preventative controls, log sources, and optimize log costs. BlueVoyant can also provide a high level of expertise to assist with a complete migration from a legacy SIEM for an additional cost.
- Three SecOps FTEs spend two hours a week supporting implementation, which spans across eight weeks.
- The average fully-burdened hourly salary of a SecOps FTE is $68.50.

- The director of cyber security also spends 10 hours per week over eight weeks on implementation.
- The average hourly fully-burdened salary of a director of cyber security is $100.
- An additional seven SecOps FTEs are trained on BlueVoyant. On average, training requires 16 hours per SecOps FTE.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Number and roles of FTEs involved in implementation.
- Average salaries of FTEs involved in implementation.
- Number of FTEs trained on BlueVoyant.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $76,000.

> "The initial training is mostly self-explanatory. It depends on the level of the analyst or the level of the security. I would say they're fully trained on everything within a week or two."
>
> CISO, MANUFACTURING

Implementation And Training Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	BlueVoyant deployment fee	Composite	$50,000			
E2	SecOps FTES supporting implementation	Composite	3			
E3	Hours spent per week on implementation	Composite	2			
E4	Length of implementation (weeks)	Composite	8			
E5	Average hourly fully-burdened salary of a SecOps FTE	Composite	$68.50			
E6	**Subtotal: SecOps FTE internal implementation costs**	**E2*E3*E4*E5**	**$3,288**			
E7	Hours a director of cybersecurity spends per week supporting implementation	Composite	10			
E8	Average hourly fully-burdened salary of a director of cyber security	Composite	$100			
E9	**Subtotal: Implementation labor cost**	**E4*E7*E8**	**$8,000**			
E10	Additional SecOps FTEs trained on solution	Composite	7			
E11	Hours of training required	Composite	16			
E12	**Subtotal: Initial training labor cost**	**E5*E10*E11**	**$7,672**			
Et	Implementation and training costs	E1+E6+E9+E12	$68,960	$0	$0	$0
	Risk adjustment	↑10%				
Etr	Implementation and training costs (risk-adjusted)		$75,856	$0	$0	$0
Three-year total: $75,856			**Three-year present value: $75,856**			

ONGOING MANAGEMENT COSTS

Evidence and data. Ongoing management involves regular check-ins, reporting, and collaboration with the BlueVoyant team. Interviewees noted that these check-ins offered valuable and strategic insights for their organization's security program.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Three SecOps FTEs support ongoing management of BlueVoyant. On average, they spend 24 hours per year.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Number of SecOps FTEs supporting ongoing management.
- The average hourly fully-burdened salary of a SecOps FTE.

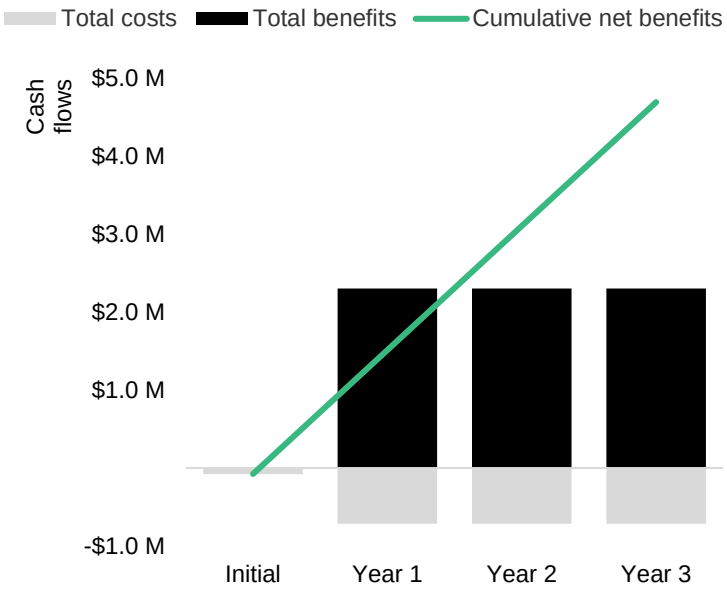
Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $13,000.

Ongoing Management Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	SecOps FTEs supporting ongoing management	Composite		3	3	3
F2	Hours spent on ongoing management annually	Composite		24	24	24
F3	Average hourly fully-burdened salary of a SecOps FTE	Composite		$68.50	$68.50	$68.50
Ft	Ongoing management costs	F1*F2*F3		$4,932	$4,932	$4,932
	Risk adjustment	↑10%				
Ftr	Ongoing management costs (risk-adjusted)		$0	$5,425	$5,425	$5,425
	Three-year total: $16,276			**Three-year present value: $13,492**		

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	($75,856)	($714,175)	($714,175)	($714,175)	($2,218,382)	($1,851,904)
Total benefits	$0	$2,304,888	$2,304,888	$2,304,888	$6,914,665	$5,731,916
Net benefits	($75,856)	$1,590,713	$1,590,713	$1,590,713	$4,696,283	$3,880,012
ROI						210%
Payback period (months)						Less than 6

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."

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.

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.

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] This cost is inclusive of average remediation and reporting labor costs, average costs of response and notification, fines, damages, compliance costs, customer compensation, average lost business revenues and additional costs to acquire customers, and end-user downtime as it relates to a security breach across the organization. Forrester Consulting conducted an online survey of 351 cybersecurity leaders at global enterprises in the US, the UK, Canada, Germany, and Australia.

Survey participants included managers, directors, VPs, and C-level executives who are responsible for cybersecurity decision-making, operations, and reporting. Questions provided to the participants sought to evaluate leaders' cybersecurity strategies and any breaches that have occurred within their organizations. Respondents opted into the survey via a third-party research panel, which fielded the survey on behalf of Forrester in November 2020. Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021.

FORRESTER®