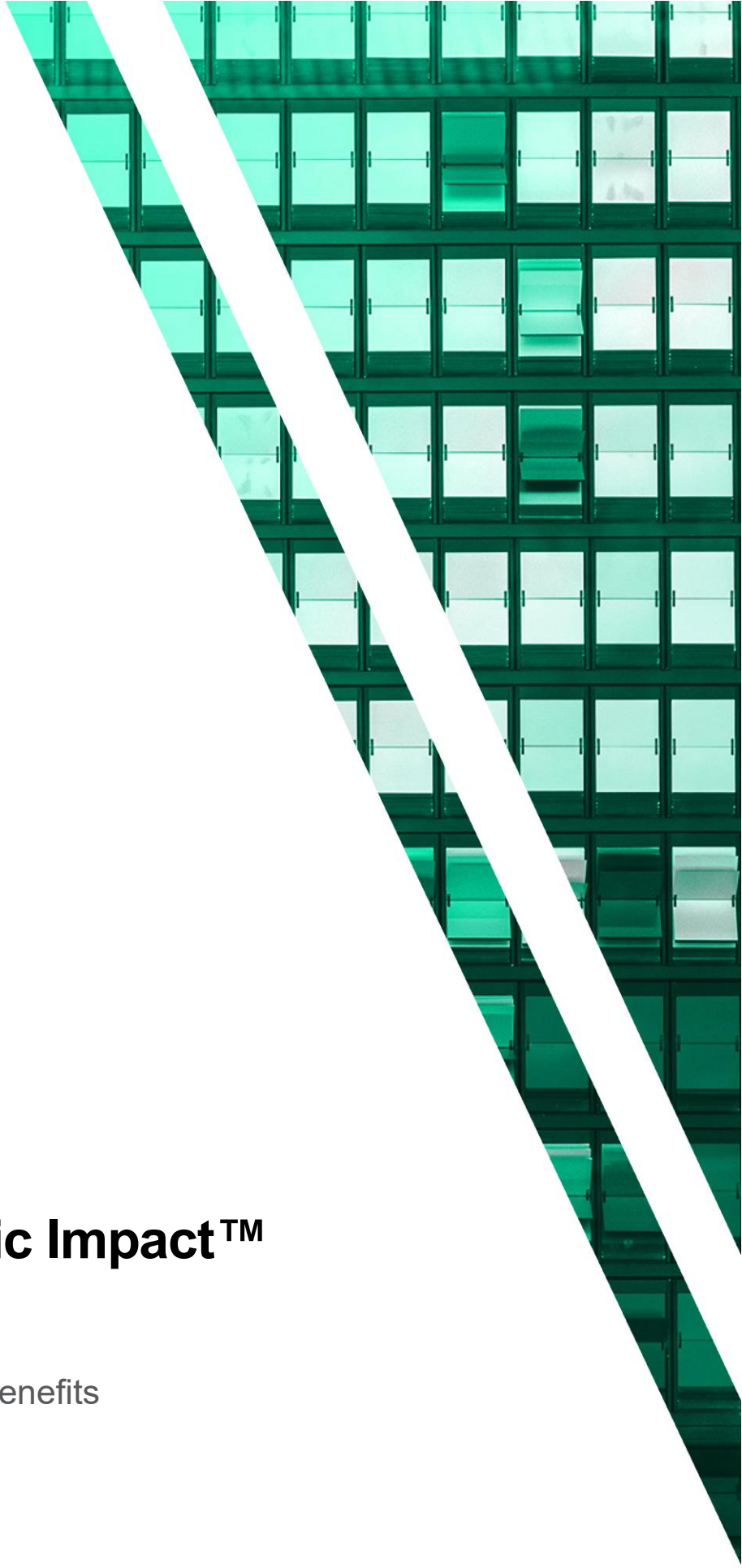
FORRESTER®



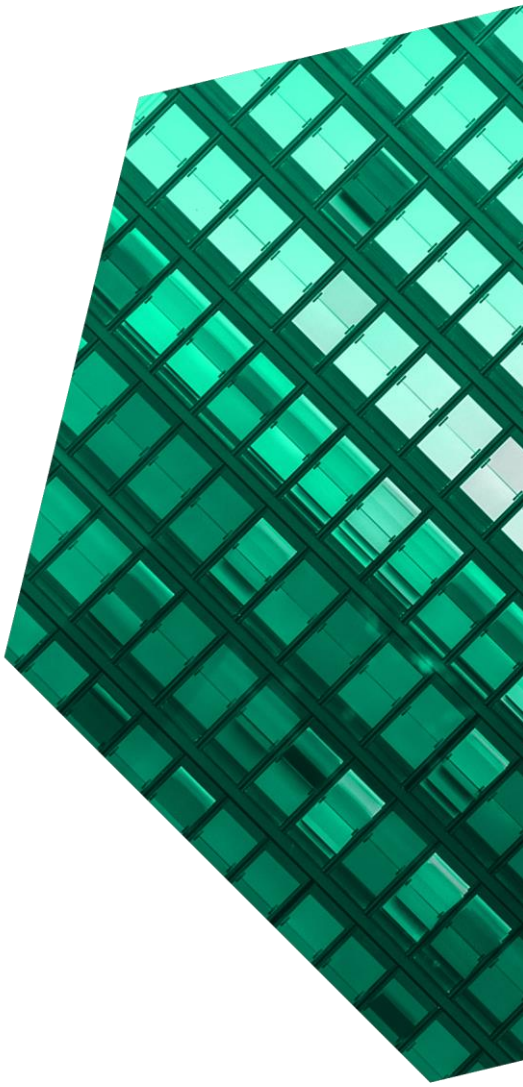
The Total Economic Impact™ Of XM Cyber

Cost Savings And Business Benefits Enabled By XM Cyber

SEPTEMBER 2022

Table Of Contents

Consulting Team: Eric Hall



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.

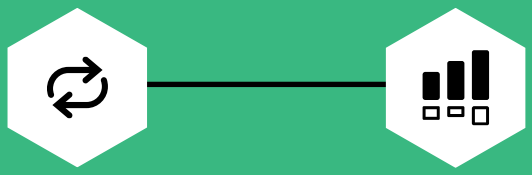
Executive Summary

As the emphasis on cybersecurity becomes more centerstage there is a greater awareness that protecting the organization's crown jewels from sophisticated bad actors requires constant identification and remediation of the most critical cyber exposures and how they combine together across these environments to put critical assets at risk. XM Cyber provides continuous and proactive security posture management across cloud and on-premises environments and automatically identifies exploitable attack paths.

XM Cyber solution maps an organization's on-prem and cloud environments to identify exploitable attack paths that bad actors utilize to reach and compromise critical business assets and offers prioritized remediation that improves its security posture. XM Cyber visualizes how the combination of technical weaknesses such as vulnerabilities, misconfigurations, identity exposures, and user behavior could be exploited by an attacker to breach critical business assets. Identifying the high-priority attack vectors and attack paths reduces risk and has the added benefit of reducing overall remediation efforts because lowly scored risk security issues may be deprioritized. XM Cyber utilizes cloud APIs and sensors that perform without device outages, disruptions, or performance issues, which allows scenarios to be run constantly — unlike ad hoc penetration testing (i.e., pen testing), to effectively monitor the ever-changing attack surface due to the dynamic nature of modern infrastructure. In addition to reducing the frequency of breaches and the average cost of breaches, XM Cyber enables customers to save money by reducing the regular need for pen testing and by reducing the need to perform patching of assets with low vulnerability.

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

KEY STATISTICS



Return on investment (ROI)
394%

Net present value (NPV)
$11.60M

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using XM Cyber. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that has 15,000 devices and a mature security operations center (SOC).

These interviewees noted that prior to using XM Cyber, their organizations prioritized device patching based upon individual asset vulnerabilities and assets identified during focused pen testing, which is infrequent, expensive, and often disruptive to devices in production.

After the investment in XM Cyber, the interviewees' organizations prioritize device patching and remediation of security issues based upon exposed

assets within cyber kill chains. In addition to better prioritization, the relationship between IT operations (IT ops) and cybersecurity improved because XM Cyber provides details on its findings, which leads to better trust by IT ops as well as a basis for better communications. Other results include the ability to reduce pen testing and the ability to reduce patching to assets that put the most critical surfaces at risk.

KEY FINDINGS

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

- **Avoided costs of remediation, fines, customer costs, revenue lost, and brand rebuilding of $12.4 million over three years.** The composite organization reduces the frequency and severity of cybersecurity attacks by utilizing XM Cyber to prioritize a focus on security exposures and remediation activities on issues associated with critical assets.
- **Penetration testing cost reduction of $1.4 million over three years.** The composite organization reduces pen testing costs while staying in compliance with regulatory requirements. External and internal resources are reduced.
- **Labor cost reduction for patching and remediation activities of $.7 million over three years.** By focusing on vulnerabilities associated with critical assets, the composite organization reduces IT patching resource efforts.

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

- **Better relationship between IT ops and cybersecurity teams.** XM Cyber's ability to provide solid and clear reasoning behind its recommendations leads to an alignment of the IT ops and cybersecurity teams.
- **Reduction in future cybersecurity pen testing and software costs.** The organization has a conservative overall security approach. It is at a comfort level with XM Cyber where it has reduced pen testing to some extent. It is also considering reducing the use of other cybersecurity software and further reducing its pen testing.
- **Reduction of risks related to working with third parties and in acquisition assessments.** XM Cyber helps reduce risk related to integrating with third parties, and the composite recommends or requires some third parties to use XM Cyber. The composite uses XM Cyber in merger and acquisition assessments.
- **Reduction of business disruption.** XM Cyber's ability to offset some pen testing reduces pen testing-related disruptions. XM Cyber's ability to identify major security exposures allows the composite to avoid certain patching or enable more flexible scheduling of patches, which reduces business disruptions due to device downtime during business hours.
- **Employee satisfaction improvement related to cybersecurity activities.** Members of both the composite's IT operations and cybersecurity teams are more excited about their jobs. Employees are aware that they are doing higher-value work, IT Ops employees resolve security issues that they can tell reduce risk, and cybersecurity teams do cybersecurity activities that provide greater strategic value.
- **Having a partner with strong communications and technical skills.** Interviewees said XM Cyber supports its customers. A director of information security, governance, and risk compliance, insurance shared: "XM Cyber has acted more like a business partner than a vendor in a lot of ways. They really helped us in a time of need, and I think there is a lot of goodwill that has been built between our organizations."

- **Improvement of communications and respect with corporate leadership and business leaders.** The composite organization makes improvements to the presentations and communications with leaders at all levels. A chief security officer and information security officer in the manufacturing industry shared: "Previously, our board was just consuming an IT security status. We now join monthly CEO-level meetings and explain important things for them to know via XM Cyber reports. They are more aware of severe threats and how we dealt with them using XM Cyber."

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

- **XM Cyber cost of $2.9 million over three years.** The composite pays costs for implementation, building attack scenarios, and licensing associated with 15,000 devices.

The representative interviews and financial analysis found that a composite organization experiences benefits of $14.54M over three years versus costs of $2.94M, adding up to a net present value (NPV) of $11.60M and an ROI of 394%.

Voices From Representatives Of Comparatively Mature Security Organizations

"We had a quite good [security] maturity prior to XM Cyber. We are now much, much safer and secure than we were in the past. I'm absolutely convinced that we see much more in detail where our biggest exposures are now."

- *Chief security officer and information security officer, manufacturing*

"As you would expect, [a bank is] quite strong at managing risk and cyber itself. Today, we are easily in the best place we've ever been. XM Cyber has been a significant factor."

- *Cybersecurity leadership, financial services*

"XM Cyber has highlighted some complexities in our environment which led to our simplifying some things while bolstering other things. It has had an impact on how we approach identity and access management to bolster our vulnerabilities and threat-posture management."

- *Director of information security, governance, and risk compliance, insurance*

"In the retail business, you have a lot of life cycle problems because you try to run hardware as long as possible. For patch management and vulnerability, this is really a big problem. With pen testing, we had a lot of outages because of the scanning; it can be very intrusive. We found XM Cyber's sensors to be nonintrusive [and] leading to no outages or performance issues [after] having deployed over 180,000 sensors."

- *Head of IT infrastructure, retail*

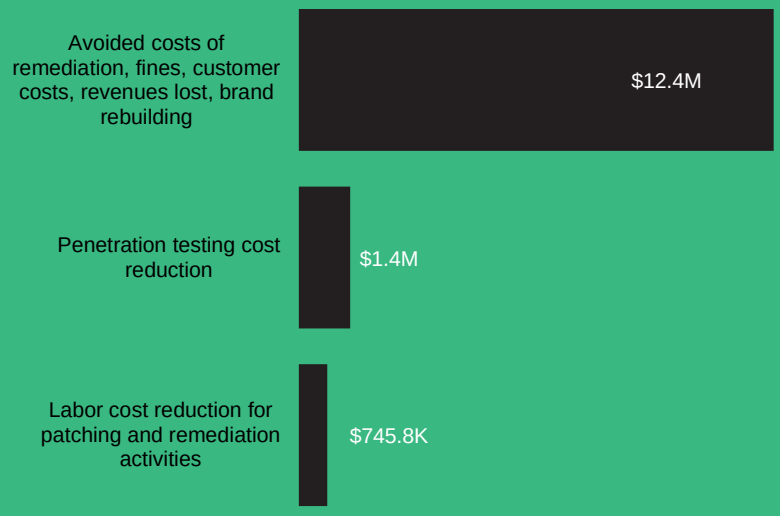
ROI
394%

BENEFITS PV
$14.54M

NPV
$11.60M

PAYBACK
<6 months

Benefits (Three-Year)



“Pen tests are about protecting the castle from penetration while XM Cyber is about protecting the crown jewels from being stolen. The focus has shifted to protecting the crown jewels.”

— Director of information security, governance, and risk compliance, insurance

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 XM Cyber.

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 XM Cyber can have on an 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.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by XM Cyber 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 XM Cyber.

XM Cyber 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.

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

The XM Cyber Customer Journey

Drivers leading to the XM Cyber investment

Interviews			
Role	**Industry**	**Region**	**Device count**
Cybersecurity leader	Financial services	Europe	10,000
Chief security officer and information security officer	Manufacturing	Global	20,000
Director of information security, governance, and risk compliance	Insurance	United States	5,000
Head of IT infrastructure	Retail	Global	300,000

KEY CHALLENGES

All four interviewees considered their organizations' cybersecurity organizations to be quite mature prior to implementing XM Cyber, but they had similar challenges. First, they wanted to make sure they kept up with the bad actors who are constantly getting better at causing harm. Second, pen testing is done too infrequently due to the cost, disruption, and effort involved in doing it. Third, they knew that they can't remediate all security soft spots, so prioritizing remediation based upon exposures that put critical assets at risk was crucial. Finally, as the organizations change, such as by expanding into the public cloud, they want to know that they are covering new exploitable pathways.

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

- **Cybercriminals keep getting better and are acting more frequently.** The interviewees noted that they must work hard to keep one step ahead of bad actors because they are constantly working to find new ways to perform cyberattacks. As a cybersecurity leader from a financial services company described it: "One [type of] organization that does innovation extremely well is cybercriminal organizations. From the defending perspective, innovating and improving is not an option; it's a necessity. We're always looking for how we can do things effectively quicker, faster, [and] better. That is why we went into this world of security posture management with XM Cyber."
- **Other than penetration testing, other solutions evaluate individual assets without effectively evaluating pathways and the relationship to critical assets.** The cybersecurity leader from the financial services company said: "Our EDR (endpoint detection and response) system keeps improving, which is really good. The problem is that its data points exist within silos, and that isn't good enough."

> **"We do a lot of work getting the fences higher and higher. We have market leader products. We always had slippages in terms of defending. We were missing some preventative things."**
>
> *Head of IT infrastructure, retail*

“My problem with pen testing was that we only did testing of our critical equipment once a year. It gives you a feel-good sensation for about a month. What I wanted to do in this space was to have greater coverage more frequently. I couldn’t solve this by throwing people at it.”

Cybersecurity leader, financial services

- **Penetration testing is only done periodically due to cost, business disruption, and labor requirements.** All interviewees spoke of the need for some level of pen testing to thoroughly evaluate their organizations’ internal and external networks for cyber exposures. Although the findings provide valuable insights towards establishing better cybersecurity measures, pen testing is done infrequently due to disruptions caused by outages or performance issues, labor efforts for planning and execution, and the common cost of external pen testing experts.
- **A constantly changing IT infrastructure creates new paths and opportunities for cybercriminal attacks.** Interviewees spoke of their organizations’ ever-changing infrastructures, with public clouds, hybrid environments, and internet-of-things (IoT) devices leading to additional entry points and paths to reach critical infrastructures. The director of information security, governance, and risk compliance at an insurance organization shared: “There was a variety of growing needs within the detection, response, and remediation components of the security team that really needed to be bolstered as the firm expanded our use of the public cloud. XM Cyber was brought in to help with cloud posture management and vulnerabilities that appear within our environment.”
- **Interviewees spoke of always having a constant list of thousands to hundreds of thousands of patches.** They felt that it wasn’t possible to complete all patches, so focusing on resolving vulnerabilities that provide a path to critical infrastructure was a higher priority than prioritizing patches based on individual device vulnerabilities.

“Trying to prioritize around 100,000 actions makes one wonder where to focus our energy. I really wanted to make sure that whenever we’re placing money in places and people in places, we’re doing it in a very intelligent way.”

Cybersecurity leader, financial services

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees’ organizations searched for a solution that could:

- Provide an automated methodology to frequently analyze the security exposures across the organization’s entire infrastructure without outages, disruptions, or performance issues.
- Understand cyberattack pathways and identify security issues creating the greatest exposure to critical infrastructure.
- Provide out-of-the-box scenario analyses as well as custom scenarios based upon unique

customer experiences or specific threats, such as malware or zero-day vulnerabilities.

- Reduce the requirement for other vulnerability management activities, most notably pen testing.

After a proof of concept (POC), the interviewees' organizations chose XM Cyber and began deployment.

- Three out of four interviewees said their organization chose to do a POC, and all three organizations identified possible security vulnerabilities that led to immediate remediation activities. The chief security officer and information security officer in the manufacturing industry described their organization's POC like this: "It took only four weeks to prove to us how beneficial XM Cyber is. The IT ops people were really surprised about the results. They saw how it helps to identify assets and the biggest threats. We deployed about 200 sensors — which is over 1% of our network — and, from the beginning, we saw real threats and that some of our existing assessments were completely wrong. We immediately started remediations, ran the same scenarios again, and saw the positive impact on the threats."

"Coincidentally, we were being haunted by the PrintNightmare vulnerability when we did the XM Cyber POC. XM Cyber identified that our virtual desktop's golden image was reintroducing it with each installation. It was easy to fix, but not easy to find. This was an eye-opener for my team."

Chief security officer and information security officer, manufacturing

- A common concern that led to a POC was whether XM Cyber's sensors would cause outages or performance issues. The interviewees' organizations found little to no performance overhead with the sensors either in the POC or in production. The head of IT infrastructure at a retail organization shared: "We knew that they would have these agents sniffing around, and we had concerns related to both privacy and performance. The POC proved to us that the sensors wouldn't be a problem from an outage or performance standpoint. XM Cyber was transparent in terms of certifications that they have and what the sensors do, so we knew that there were no privacy issues."

"We had the sensors all independently profiled by a third party. They monitored XM Cyber from a functionality perspective and by its effect on our performance. There were no findings of concern."

Cybersecurity leader, financial services

- Interviewees spoke of performing the POCs for a shorter time than originally planned because XM Cyber proved itself quickly. The cybersecurity leader in financial services described what convinced their organization to implement XM Cyber: "As part of our POC we simulated ransomware. We thought that we were impervious to a serious ransomware attack due to our great layers of defense. [XM Cyber] ultimately came across one particular individual who was running as administrator, and it turned

out that he wasn't just admin on one box — he was admin on a lot of boxes and, subsequently, those additional rights and access that he had meant that this one person could actually make a change to every box in the bank. XM Cyber found one person who could have [made] the entire organization fall."

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. The composite organization had a relatively mature SOC that had vulnerability management software before adding XM Cyber's solution. The organization has a large financial exposure to having a breach, be it critical assets, brand reputation exposure, a highly targeted industry, or some other significant risk.

The composite organization has 15,000 devices spread between multi-location on-premises infrastructure and multiple cloud services. There is a large cybersecurity team with pen testing required due to regulations and due to internal requirements to protect critical infrastructure.

Key Assumptions

- **Mature cybersecurity team**
- **15,000 devices**
- **On-premises and multiple clouds**
- **Annual external penetration testing cost of $500,000**
- **8 FTEs for penetration testing**
- **15 FTEs for patching and remediation**

"To be honest, I originally wanted the solution provided by a current vendor [because it would be] one less tool to manage. But XM Cyber definitely came out on top. It works like a car navigation system algorithm, but you don't want it to find the route from point A to point B. If it finds a pathway, then it explains the vulnerabilities. [It's] not what you want to hear, but at least I can pick it apart to make it safe."

Cybersecurity leader, financial services

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	Avoided costs of remediation, fines, customer costs, revenues lost, brand rebuilding	$5,004,604	$5,004,604	$5,004,604	$15,013,812	$12,445,710
Btr	Penetration testing cost reduction	$488,000	$576,000	$576,000	$1,640,000	$1,352,427
Ctr	Labor cost reduction for patching and remediation activities	$243,000	$303,750	$364,500	$911,250	$745,796
	Total benefits (risk-adjusted)	$5,735,604	$5,884,354	$5,945,104	$17,565,062	$14,543,933

AVOIDED COSTS OF REMEDIATION, FINES, CUSTOMER COSTS, REVENUES LOST, BRAND REBUILDING

Evidence and data. Though their organizations were already quite mature at vulnerability and security posture management, interviewees' organizations used XM Cyber to reduce the frequency and damages of breaches. Most notably, this was accomplished by frequent, automated attack scenarios run across internal and external networks that identified critical asset threats.

- Interviewees described XM Cyber going through a network learning activity, identifying pathways to critical assets combining exposures that put those assets at risk. The pathways may have been on-premises, within a cloud, across clouds, or hybrid. The director of information security, governance, and risk compliance at an insurance organization said: "XM Cyber provides a single-pane dashboard where you can see those lateral movements and really understand how an attacker might move within your environment from a north-south, east-west perspective. You can see how they might jump from system to system, making lateral or vertical moves. It pokes and prods across the entire environment rather than just [in] one stove pipe."

"We had a situation where a DevOps guy was storing a bunch of keys on his laptop, which is a huge security concern. XM Cyber came along, found all these keys on his laptop, and determined that 80% of our infrastructure could be owned if those keys were accessed."

Director of information security, governance, and risk compliance, insurance

- Interviewees said their organizations set up their own scenarios (also called simulations or abuse cases) that identify threats like ransomware, cloud integration threats, complex domain credential threats, or areas of architecture that may degrade over time. The chief security officer and information security officer at a manufacturing company said, "Threats associated with domain credentials can be very complex, so we have scenarios in place to identify these risks." The director of information

security, governance, and risk compliance at an insurance company shared, “One of the most valuable features is finding cyberkill chains by setting up attack simulations that can run the integration into our cloud environments and look at the cloud posture.”

“When we have seen a lot of choke points and issues in a certain area, we take this as an opportunity to look at that kill chain and the chokepoints and consider how we might change how we're operating to help mitigate or reduce this area of concern. We have had quick wins and have built up our security posture quickly.”

Director of information security, governance, and risk compliance, insurance

- Interviewees’ organizations ran these scenarios constantly with no outages or degradation common from pen testing. The director of information security, governance, and compliance in the insurance industry shared, “A pen tester is looking at certain aspects at a point in time that become stale about 30 days later, while XM Cyber is all-encompassing and continues to provide findings year-round.”
- Findings were used to prioritize remediation activities on higher-impact security vulnerabilities that were putting critical infrastructure at risk. Interviewees described XM Cyber’s ability to identify critical exposures and effectively communicate the significance of the risk.
- Since scenarios were run constantly, new security issues were identified quickly, and failed or incomplete remediation was surfaced and rectified in a short timeframe. The head of IT infrastructure in the retail industry explained: “Since scenarios are run constantly, we’re able to go back and ensure that the remediation effort was accomplished successfully. It is not uncommon to catch patches that weren’t done right.”

“Every company in the world has too many vulnerabilities to manage, and you get this alert fatigue, so you don’t even know where to start. In some areas, we have 200,000 patches in the queue. But with XM Cyber, we see the most vulnerable points.”

Head of IT infrastructure, retail

Modeling and assumptions. To calculate the value of this benefit, Forrester assumes the following:

- According to Forrester Consulting’s Cost Of A Cybersecurity Breach Survey, Q1 2021, the composite organization experiences an average of 4.1 breaches per year for an organization of this profile.[2] This data is used for the number of breaches per year at a typical maturity level, the average cost per data breach of $2,145,983 exclusive of internal user downtime, and assumes that 79% of breaches are associated with the security space covered by XM Cyber.

- The composite organization's likelihood of a breach for the security space that XM Cyber covers is reduced by 90%.

Risks. Risks that could impact the realization of this benefit include:

- The maturity of the cybersecurity team.
- Specific industries, companies, and global regions, which see different levels of threats.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $12.4 million.

Avoided Costs Of Remediation, Fines, Customer Costs, Revenues Lost, Brand Rebuilding

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Average number of breaches annually	Forrester research	4.1	4.1	4.1
A2	Average potential cost of data breach, exclusive of internal user downtime	Forrester research	$2,145,983	$2,145,983	$2,145,983
A3	Percentage of cyber security covered by XM Cyber	Forrester research	79%	79%	79%
A4	Reduction in likelihood of a severe breach due to XM Cyber's cyber security coverage	Composite	90%	90%	90%
At	Avoided costs of remediation, fines, customer costs, revenues lost, brand rebuilding	A1*A2*A3*A4	$6,255,755	$6,255,755	$6,255,755
	Risk adjustment	↓20%			
Atr	Avoided costs of remediation, fines, customer costs, revenues lost, brand rebuilding (risk-adjusted)		$5,004,604	$5,004,604	$5,004,604
	Three-year total: $15,013,812			**Three-year present value: $12,445,710**	

PENETRATION TESTING COST REDUCTION

Evidence and data. The interviewees' organizations were able to provide constant scenario simulations with XM Cyber, reducing pen testing activities, either by reducing the use of external resources or by reducing a combination of internal and external resources. Interviewees also found XM Cyber to be less intrusive, not causing outages or performance issues that commonly occurred during pen testing.

Modeling and assumptions. To calculate the value of this benefit, Forrester assumes the following:

- The composite organization's outside cost for pen testing is $500,000 per year.
- Outside pen testing costs are reduced by 50% in Year 1 and by 60% in subsequent years.

> **"We had seven FTEs on pen testing with the assistance of contractors at about $500,000 per year. We are doing the equivalent pen testing work with 1.5 FTEs and $100,000 externally to get an outside perspective."**
>
> *Cybersecurity leader, financial services*

- The composite organization's internal labor requirement for pen testing is eight FTEs.
- Internal labor for pen testing is reduced by 60% in Year 1 and by 70% in subsequent years.

- The labor recapture rate is 50%
- The fully loaded labor cost of a security team member is $150,000 per year.

Risks. Risks that could impact the realization of this benefit include:

- The complexity of the network infrastructure and the associated need for outside expertise.
- Variance in regulation requiring penetration testing.
- The internal compliance requirements for penetration testing.
- Variance in labor costs.
- The skills of the internal security team and the extent that resources are shifted to higher-value security activities.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $1.4 million.

Penetration Testing Cost Reduction

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Pen testing - outside cost	Composite	$500,000	$500,000	$500,000
B2	Outside cost reduction (percent)	Interviews	50%	60%	60%
B3	Subtotal: Pen testing external cost reduction	B1*B2	$250,000	$300,000	$300,000
B4	Pen testing - internal team (FTEs)	Composite	8	8	8
B5	Pen testing - internal FTE reduction	Interviews	60%	70%	70%
B6	Pen testing - internal FTE recapture	Interviews	50%	50%	50%
B7	Fully loaded annual labor cost for SOC team member	TEI standard	$150,000	$150,000	$150,000
B8	Subtotal: Pen testing internal cost reduction	B4*B5*B6*B7	$360,000	$420,000	$420,000
Bt	Penetration testing cost reduction	B3+B8	$610,000	$720,000	$720,000
	Risk adjustment	↓20%			
Btr	Penetration testing cost reduction (risk-adjusted)		$488,000	$576,000	$576,000
	Three-year total: $1,640,000			**Three-year present value: $1,352,427**	

LABOR COST REDUCTION FOR PATCHING AND REMEDIATION ACTIVITIES

Evidence and data. The interviewees' organizations have been able to focus on vulnerabilities that are associated with critical infrastructure. Two organizations chose to reduce patching resources based upon the combination of individual vulnerabilities and vulnerabilities tied to critical asset threats.

> **"We reduced the number of FTEs doing patching by 20% while also doing a better job."**
>
> *Head of IT infrastructure, retail*

Modeling and assumptions. To calculate the value of this benefit, Forrester assumes the following:

- The composite organization has 15 patching and remediation team members.
- The patching and remediation team is reduced by 20% in Year 1 and by another 5% each year.
- The fully loaded labor cost of a patching and remediation team member is $90,000 per year.

Risks. Risks that could impact the realization of this benefit include the strategy of balancing labor costs and overall risk reduction through patching.

- The amount of patching required for non-security related purposes.
- Labor costs will vary.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $0.7 million.

Labor Cost Reduction For Patching And Remediation Activities

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Patching and remediation teams (FTEs)	Composite	15	15	15
C2	Patching and remediation teams reduction	Interviews	20%	25%	30%
C3	Fully loaded annual labor cost for IT operations staff member	TEI standard	$90,000	$90,000	$90,000
Ct	Labor cost reduction for patching and remediation activities	C1*C2*C3	$270,000	$337,500	$405,000
	Risk adjustment	↓10%			
Ctr	Labor cost reduction for patching and remediation activities (risk-adjusted)		$243,000	$303,750	$364,500
	Three-year total: $911,250			**Three-year present value: $745,796**	

UNQUANTIFIED BENEFITS

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

- **IT ops and cybersecurity teams work better together.** Interviewees shared that XM Cyber's ability to provide solid and clear reasoning behind its recommendations has led to an alignment of IT ops and cybersecurity teams. The chief security officer and information security officer in the manufacturing industry said: "A huge benefit for me right now is that there's no competition between IT security and IT operations anymore. IT operations uses XM Cyber proactive now. The

"We are having more meaningful conversations with IT operations because we are able to lay out what vulnerabilities that we should be addressing, and we get their buy-in. We may show them that we don't have compensating controls in certain areas, so new priorities are needed."

Director of information security, governance, and risk compliance, insurance

people responsible for servers, for example, have set up some of their own scenarios and solve problems better than in the past. People see that their actions make their responsible area more secure. Things are much better now."

- **Reduced business disruption.** Interviewees shared that XM Cyber's ability to offset some of the pen testing has reduced pen testing-related disruptions. XM Cyber's ability to identify major vulnerabilities has allowed them to avoid certain patching or enable more flexible scheduling of patches, which has reduced business disruptions due to device downtime during business hours. The head of IT infrastructure in retail said: "We have thousands of stores around the world with many components per store, so it is a huge task to deal with vulnerabilities. By focusing on the critical vulnerabilities, we are not broadly scheduling downtimes for patches. There are huge time savings both within my team and within the stores."

"We did a lot of penetration tests trying to get underneath and detect things, but this is a very time-consuming task. We had a lot of outages because of the scanning; it was a very intrusive thing."

Head of IT infrastructure, retail

- **Reduction in future cybersecurity pen testing and software costs.** Interviewees' organizations have been conservative with their overall security approaches. They have reached a comfort level with XM Cyber's use to reduce pen testing, but interviewees said their organizations were only considering reducing the use of other cybersecurity software and further reducing their pen testing at the time of the interviews.
- **Reduced risks related to working with third parties and in acquisition assessments.** Interviewees described how XM Cyber is helping their organizations reduce risk related to integrating with third parties as well as recommending or requiring some third parties to use XM Cyber themselves. Interviewees also described using XM Cyber as part of their evaluations of potential merger and acquisition assessments. The head of IT infrastructure in the retail industry shared: "If a company exclusively supports us, then we can require that they use XM Cyber. But if they support many companies, then we look for the opportunity to discuss XM Cyber's value with them."

"I measure risk reduction by how long I can sleep. I sleep better now."

Head of IT infrastructure, retail

- **Employee satisfaction improvement related to cybersecurity activities.** Interviewees shared that both IT operations and cybersecurity team members are more excited about their jobs. Employees are aware that they are doing higher-value work, IT ops employees are resolving issues that they can tell reduces risk, and cybersecurity team members are doing cybersecurity activities that provide greater strategic value. Interviewees even spoke of the possibility that having XM Cyber may benefit their organizations in recruiting and retaining quality cybersecurity analysts. The cybersecurity leader in the financial services industry said: "We can retain and recruit people better because our current roles are things that people want to do. I

am quite optimistic for the future because having happier people will be a differentiator for us."

- **Having a partner with strong communications and technical skills.** Some interviewees' quotes tell the story of XM Cyber's relationship with and support of its customers. The head of IT infrastructure in retail spoke highly of the XM Cyber team's technical and soft skills. They said: "These guys are exceptional in terms of … quality from a technical perspective. They also have been quite good in terms of how [they] interact with my people."
- **Improved communications to and respect of corporate leadership and business leaders.** Interviewees spoke of improvements that have occurred with their presentations and communications with leaders at all levels within their organizations. The cybersecurity leader in the financial services industry shared: "The XM dashboards are very useful. One dashboard, video playthrough of how things transfer through the network and the technique being used at the time, looks very *Matrix*-esque, and it has an incredibly powerful effect when you put it in front of the business." The head of IT infrastructure in the retail industry said: "We present XM Cyber dashboards to our board to show our performance. The dashboards are so well done that we are considering providing some board members with the ability to view XM Cyber dashboards on their screens."

"Our security team is far more excited about doing more red-team, high value activities than they are about discovering missed patches and misconfigurations, which are now largely taken care of by XM Cyber. By taking away the low-level tasks I find that they are also working smarter, focusing on business objectives that bleed into a broader scope that leads to better work."

Cybersecurity leader, financial services

FLEXIBILITY

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

- **Having the ability to respond to a new threat or turn a thought into a scenario no longer takes a team, a plan, and significant time to build, test, and execute.** Interviewees' organizations created scenarios for known abuse cases and hypothetical ones. The ease of creating scenarios supports them when new vulnerabilities are identified or as ideas on possible threat paths are being considered. Previously, testing required far more resources and time to perform.

"I can derive a question right now and probably have the answer in 15 minutes. I can do it without a test plan, change control network access, and someone spending a week doing the test."

Cybersecurity leader, financial services

- **Expanding beyond cybersecurity from an IT operations perspective to include developer hygiene management.** The director of information security, governance, and risk compliance in the insurance industry said: "We're also able to cover cybersecurity more directly from a software development standpoint, ensuring microservices and containers are secured appropriately, and we have good identity and access management policies going on. We're using privilege checks and management in the right places."

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

Voice Of The Customer: Prioritizing Remediation To At-Risk Pathways

"The bottleneck is remediation because someone must patch. XM Cyber helps us to use our resources much better than we did in the past by focusing on our key assets."
- *Chief security officer and information security officer, manufacturing*

"Statistics showed that 98% of breaches occurred from a combination of three things: missed patching, misconfiguration, and credential abuse. Cybercriminals are taking advantage of toxic combinations. XM Cyber tells me what to fix to keep [my organization] safe."
- *Cybersecurity leader, financial services*

"XM Cyber really helps you articulate the bang for your buck in terms of remediation efforts and managing resources. In this economy, nobody is working with a surplus of security [or] engineering talent. It's even more important to optimally use everyone's time right now."
- *Director of information security, governance, and risk compliance, insurance*

"We now talk about what is critical and what the timing must be, which is important in retail due to business disruptions caused by a lot of remediation activities."
- *Head of IT infrastructure, retail*

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	XM Cyber cost	$12,000	$1,182,000	$1,176,000	$1,176,000	$3,546,000	$2,941,992
	Total costs (risk-adjusted)	$12,000	$1,182,000	$1,176,000	$1,176,000	$3,546,000	$2,941,992

XM CYBER COST

Evidence and data. The interviewees said implementation of software and sensors was relatively straightforward and that licensing costs are associated with device counts.

Modeling and assumptions. To calculate this cost, Forrester assumes the following:

- The composite organization has 15,000 devices.
- The composite organization's implementation is initially $10,000. Additional scenarios are added over time, with a cost of $10,000 in Year 1 and $5,000 each for the remaining years.

Risks. Risks that could impact implementation and licensing costs include:

- The number and complexity associated with endpoints in scope.
- The cost of licensing, which may vary based upon payment terms and volume discounts.

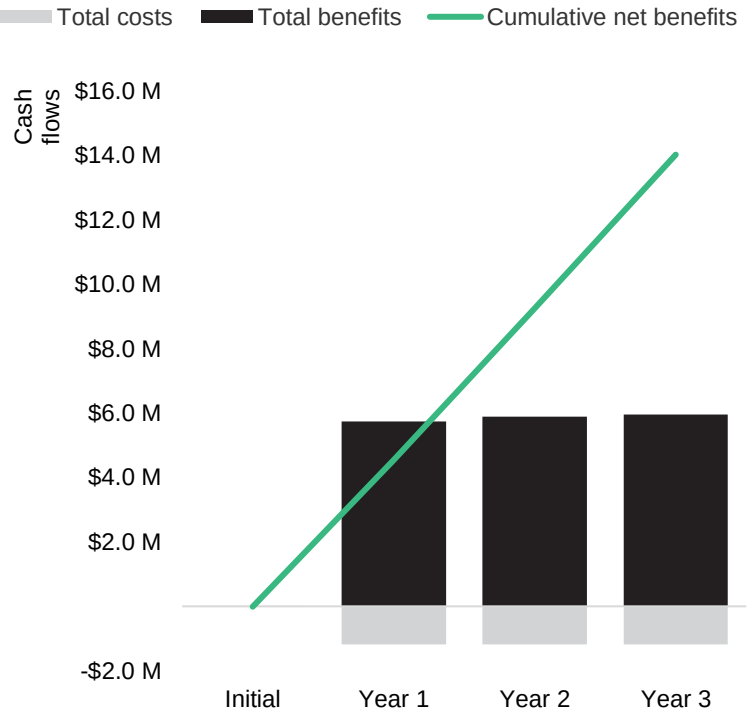
Results. To account for these risks, Forrester adjusted this cost upward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.9 million.

XM Cyber Cost						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Number of devices	Composite		15,000	15,000	15,000
D2	Licensing cost per device	Client		$65	$65	$65
D3	Implementation and building out scenarios	Client	$10,000	$10,000	$5,000	$5,000
Dt	XM Cyber cost	D1*D2	$10,000	$985,000	$980,000	$980,000
	Risk adjustment	↑20%				
Dtr	XM Cyber cost (risk-adjusted)		$12,000	$1,182,000	$1,176,000	$1,176,000
	Three-year total: $3,546,000			**Three-year present value: $2,941,992**		

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	($12,000)	($1,182,000)	($1,176,000)	($1,176,000)	($3,546,000)	($2,941,992)
Total benefits	$0	$5,735,604	$5,884,354	$5,945,104	$17,565,062	$14,543,933
Net benefits	($12,000)	$4,553,604	$4,708,354	$4,769,104	$14,019,062	$11,601,941
ROI						394%
Payback period (months)						<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."

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: Supplemental Material

Related Forrester Research
"Planning Guide 2023: Security & Risk," Forrester Research, Inc., August 23, 2022

Appendix C: Endnotes

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

[2] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021.


FORRESTER®