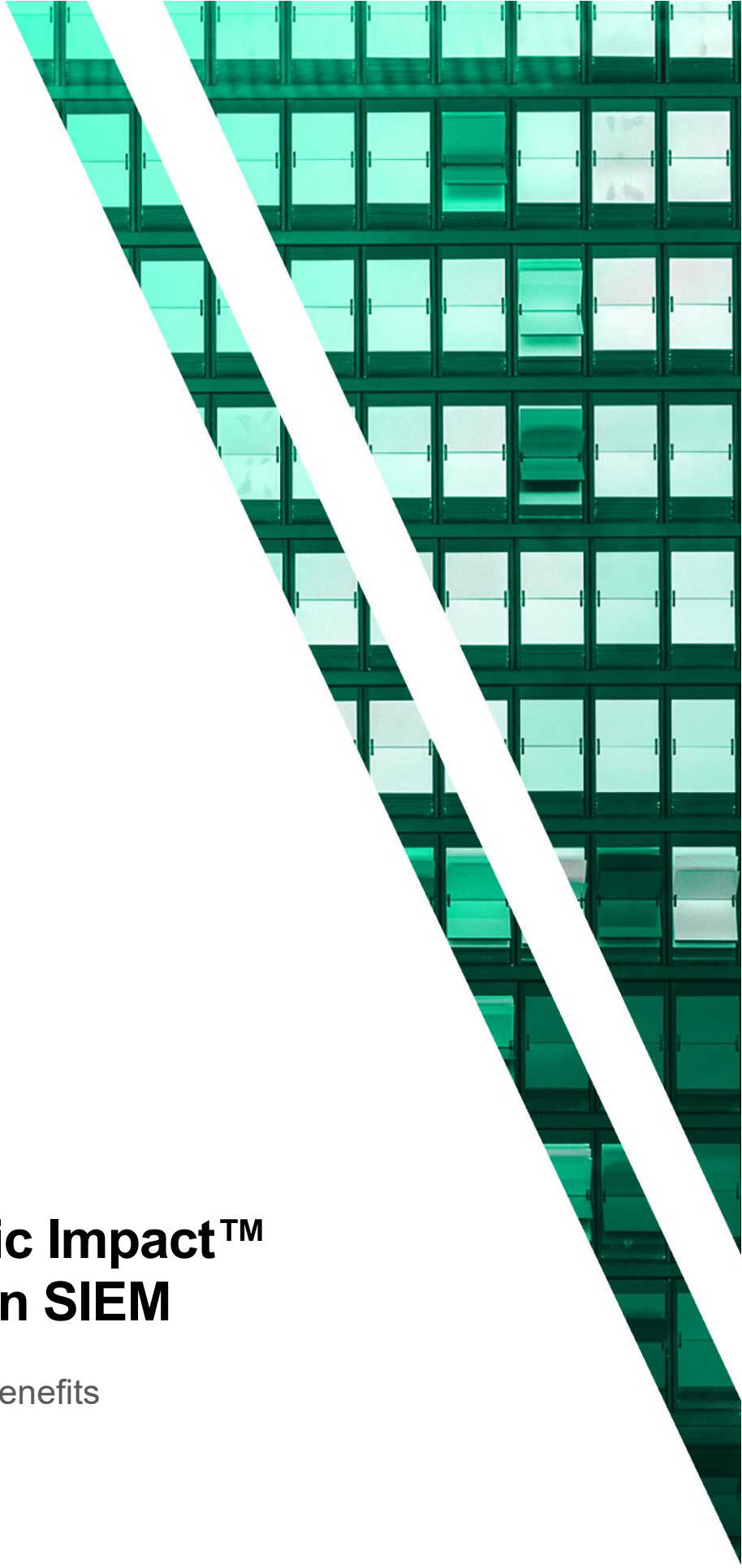
FORRESTER®



# The Total Economic Impact™ Of Exabeam Fusion SIEM

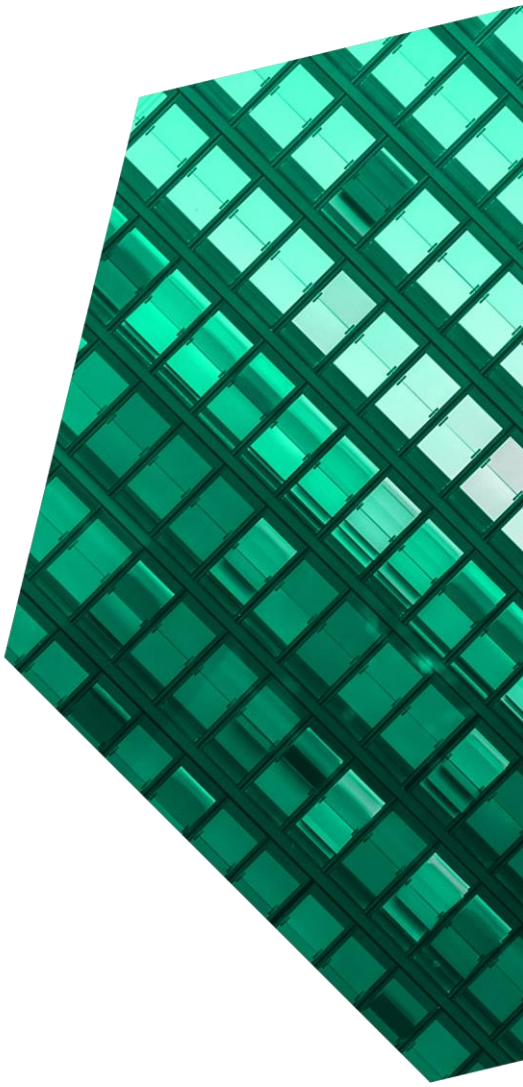
## Cost Savings And Business Benefits Enabled By Exabeam Fusion

**APRIL 2022**

# Table Of Contents




*Consulting Team: Amy Harrison*

## Executive Summary

Security teams used to have defined borders to protect, with limited user numbers and well-known threats like malware and lost or stolen laptops. As businesses evolve to embrace hybrid work policies or new technologies, the potential attack surface dramatically expands. Security professionals must defend their firm from the ever-changing attack surface with the movement of employees, customers, partners, and suppliers.[1]

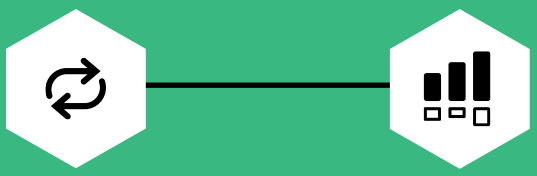
With the average security operations center (SOC) today managing nearly 20 security point products, analyst execution and team effectiveness has dropped off.[2] Despite using industry-leading tools and having complex security controls in place, organizations continue to be breached predominantly due to an inability to detect when attacks come from inside the organization or an attacker masquerades as a trusted insider. Exabeam delivers next-generation security incident and event management (SIEM) and extended detection and response (XDR) that enables organizations to modernize their SOC and eliminate their blind spots with state-of-the-art user and entity behavior analysis (UEBA)-driven threat detection, investigation, and response.

Exabeam commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Fusion SIEM.[3] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Fusion SIEM on their organizations.

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

Prior to using Fusion SIEM, these interviewees noted how the security maturity of their organizations was inconsistent with either no previous SIEM or a legacy provider that was not meeting the needs of their firm. Their legacy solutions lacked integrated workflow or workforce management functionality, causing interviewees to work inefficiently without centralized visibility. In addition, interviewees reported that security audits surfaced that these legacy SIEMs were not providing adequate visibility and detection, which drove their executives to fund additional security infrastructure.

**KEY STATISTICS**



Return on investment (ROI)
**245%**

Net present value (NPV)
**$2.65M**

Interviewees were experienced in managing storage, network, and related technology infrastructure and were familiar with the challenges of assembling and maintaining an on-premises SIEM.

Whether interviewees were replacing an existing SIEM or deploying one for the first time, they were looking for time-to-value. The regional CISO for a holding company explained, "When you don't have developers to work with, you need a simple way to bring in the data feeds. Exabeam has their Cloud

Connector, and by giving it the right credentials, it will make the API calls and pull the information for you, and then you're off to the races. The time-to-value is really affected by how fast you integrate those logs versus spending three months trying to write 12 different API calls so you can get everything going."

## KEY FINDINGS

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

- **Security team efficiency gains.** After deploying Exabeam, SOC teams gained a centralized view of their ecosystem that allowed them to quickly review and investigate security logs, alerts, and incidents. This reduced false positives and shortened mean time-to-respond and -resolve. The CISO of the mining firm reported seeing a more than 70% drop in the number of incidents their team needed to investigate, allowing them more time for threat hunting. Additionally, the CISO of the chemicals firm discussed how they could provide more security coverage with less-experienced staff.
- **Decreased financial exposure due to reduced dwell time.** Interviewees' firms previously experienced financial losses due to internal and external attacks. By deploying Exabeam, they were able to recognize and respond to threats in a matter of minutes, where previously it could have taken hours — if they were able to detect the threat at all.
- **Savings on third-party incident response services.** The electronics firm CISO had used cybersecurity incident response services (CIRS) providers for digital forensics expertise when previously hit by a cybersecurity attack. Exabeam helped them avoid spending money with these firms by allowing them to easily pull records to help in their legal defense preparation. The CISO reported saving more than $100,000 for just the investigation component for one event.
- **Cost savings from transition to the cloud.** Interviewees' on-premises solutions suffered from storage capacity and compute limitations, which are minimized in the cloud. Interviewees selected a SaaS provider because they wanted to follow their organizations' cloud-first philosophies. For others, it was about the reduced cost of system management and reduced downtime.

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

- **Reduced service-level agreement (SLA) to the business.** Leveraging Exabeam gave the IT security chief at a retail and manufacturing firm the confidence to guarantee shorter response times, allowing him to cut his SLA to the business in half.
- **Improved infrastructure team operations.** The CISO of the chemicals firm discussed how the infrastructure team uses Exabeam to provide value to their department. They used it daily to understand what might block traffic to their network applications.
- **Increased management-level visibility.** The CISO of the chemicals firm uses the metrics captured in Exabeam to stay ahead of significant changes he sees in his company's ecosystem. For example, the team tracks the number of vulnerabilities per site to understand their current security posture.
- **Eased staffing challenges.** The interviewees unanimously reported that they could operate more effectively with less-skilled employees. They worried less about employee churn and more about recruiting people with the right aptitude for the job. As a result, they could fill positions faster, with a shorter ramp time.

**Costs.** Risk-adjusted PV costs include:

- **The composite organization paid a total of $250,000 in annual fees to Exabeam.** An additional 15% of total net costs are paid to Exabeam to cover the Premier Success Plan.
- **The composite paid $75,000 in initial implementation fees.** The interviewed decision-makers told Forrester that implementation costs were both internal and external in nature, with fees paid to Exabeam and a few weeks of internal effort contributing to overall costs. Over the course of the investment, additional internal effort for training and ongoing platform maintenance cost just under $147,000.

The interviews and financial analysis found that a composite organization experiences benefits of $3.73M million over three years versus costs of $1.08M million, adding up to a net present value (NPV) of $2.65M million and an ROI of 245%.

ROI
**245%**

BENEFITS PV
**$3.73M**

NPV
**$2.65M**

PAYBACK
**<6 months**

**Benefits (Three-Year)**


**“When evaluating tools, my first two questions are, ‘Does your tool align to the NIST [National Institute of Standards and Technology] framework? Does it integrate with Exabeam?’ Exabeam became the foundation of our entire security program.”**

— CISO, mining

## 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 Exabeam Fusion SIEM.

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 Fusion SIEM can have on an organization.

### DUE DILIGENCE

Interviewed Exabeam stakeholders and Forrester analysts to gather data relative to the Fusion SIEM.

### DECISION-MAKER INTERVIEWS

Interviewed six decision-makers at organizations using Exabeam Fusion SIEM to obtain data with respect to costs, benefits, and risks.

### COMPOSITE ORGANIZATION

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

### FINANCIAL MODEL FRAMEWORK

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

### CASE STUDY

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

# The Exabeam Fusion SIEM Customer Journey

Drivers leading to the Fusion SIEM investment

| Interviewed Decision-Makers | | | |
|---|---|---|---|
| **Interviewee** | **Industry** | **Region** | **Total Employees** |
| Chief information security officer | Mining | Global | 4,900 |
| Chief information security officer | Chemicals | Global | 14,000 |
| IT security chief | Retail and manufacturing | Global | 230,000 |
| Regional chief information security officer | Holding company | Global | 40,000 |
| Chief information security officer | Electronics | Global | 6,500 |
| Head of global operations | Financial services | Global | 40,000 |

## KEY CHALLENGES

Forrester interviewed six representatives from organizations with experience using Exabeam Fusion SIEM. The interviewees described varying states of security maturity ranging from manual processing of logs with no SIEM to more mature companies that had a legacy SIEM or leveraged managed security service providers.

The regional CISO for a holding company said that until he deployed Exabeam, "security" meant mainly stopping website fraud or theft. He elaborated: "We wanted proper security in the corporate IT space. Security involved loading a bunch of software, then set it and forget it. That was security. We were not looking for internal threats or any lateral movement."

Other interviewees previously deployed a SIEM, but it was not meeting the needs of their organizations. The interviewees noted how their organizations struggled with common challenges, including:

- **Legacy solutions lacked integrated workflow or workforce management functionality.** Interviewees struggled without centralized visibility into their ecosystems. The CISO at the electronics firm described how security alerts distributed via email caused duplication of work because analysts had no way of tracking who responded to each alert. They explained: "Our previous solution just sent lots of alerts and emails. I had no visibility into my team's processing of these events. An email alert came in, and sometimes two or three agents were all working the same one. With COVID and people being remote, there was less in-office collaboration. We were operating in an ineffective state, and I needed to fix that right away."
- **Security was expanding beyond the perimeter.** The regional CISO for a holding company described how on-premises security evolved into global security. The CISO noted, "Early security efforts were based on protecting the 'perimeter' with firewalls, but there weren't devices or controls responsible for guarding the network across all business units." They realized the need for more coverage and deployed intrusion detection systems (IDS) and intrusion prevention systems (IPS). Their legacy solution didn't provide enough protection. The IT security chief continued: "We conducted two external audits: one cybersecurity maturity audit and one

that was more of a compromise assessment. We were lacking a lot of visibility and detection capabilities, which substantiated what I had been telling the business about our exposure."

**"The majority of our log collection alerting was primarily around compliance and audit. It was not about security. To be perfectly honest, we came from a very immature position where anything could've happened."**

*Head of global operations, financial services*

**Building an on-premises SIEM was a long, expensive process.** Several interviewees had extensive experience managing storage, network, and related technology infrastructure and were intimately familiar with the challenges of assembling and maintaining it. Those who attempted to build an in-house SIEM experienced challenges like an inability to scale.

**SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES**

The interviewees' organizations searched for a solution that could:

- **Deliver best-in-class security logging with ease and speed.** The head of global operations at the financial services firm was looking for a solution that would help them quickly meet regulatory requirements: "I didn't have to rely on a third-party vendor that was managing my servers, network rules, or storage. We signed the contracts, I installed some site collectors, and in a couple of days, we had logs. I mean, it was that easy. From a Fusion perspective, it was so much shorter than a traditional infrastructure build."
- **Integrate security data into a single pane of glass.** The CISO of the chemicals company sought to increase and centralize security monitoring without increasing staffing. They explained: "We're looking at everything on one screen rather than having to pull up your firewall logs and your endpoint logs from different systems with different views. It's hard to do, and Exabeam Fusion can do that. The other benefit was reduced staff requirements because we now have centralized logging, a single pane of glass for monitoring, and the alerting is very good."

**"Many companies have significant security deficiencies, and it's overwhelming to face them. You must get good control of your infrastructure to get control of your security. This allows you to work in parallel by getting up and running do some basics with the stuff you have without having to fix your entire data storage infrastructure."**

*Head of global operations, financial service*

- **Provide anomalous detection of user behavior.** The CISO of the electronics firm said: "We ended up choosing Exabeam primarily for the UEBA capability. We were really looking to operate more efficiently and do more with less resources, and we felt that Exabeam was going to give us the best coverage of behavior-based analysis." The CISO of the chemicals company

concurred: “It’s not just logging. It’s behaviors and what people do. Are people logging in from different places where they shouldn’t be logging in from — another country for instance.”

**“One thing that helped demonstrate value was the SolarWinds breach. We had to handle it as though we were compromised and dig through logs, look for indicators of compromise, and then document all that. At that time, our data retention was short. The board decided to invest to increase our log retention. That was a key event that really shaped the industry.”**

*CISO, electronics*

**COMPOSITE ORGANIZATION**

Based on the six 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 six decision-makers that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

**Description of composite.** The multibillion-dollar financial services firm provides investment services to clients across the globe. The composite organization has a strong brand, global operations, and more than 20,000 employees who live and work remotely.

**Deployment characteristics.** The composite organization has a centralized security operations center and monitors all corporate technology across all endpoints. The company outsources their level 1 SOC operations and employs eight security team members. There is one VP, two senior-level analysts, four junior-level analysts, and one intern. The composite uses SaaS-based providers for its business applications but does maintain some on-premises infrastructure. The firm chooses to deploy Exabeam in the cloud to quickly integrate its log sources without having to completely upgrade its data infrastructure. Finally, decision-makers at the composite organization choose Exabeam to maintain compliance with industry regulations.

**Key assumptions**

- **$10B+ in revenue**
- **Multiple global locations**
- **Financial services**
- **20,000 employees**
- **8 security team members**
- **Uses mostly cloud-based business apps**
- **Manages an on-premises data center**

# 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 | Security team efficiency gains | $230,230 | $230,230 | $230,230 | $690,690 | $572,548 |
| Btr | Decreased financial exposure due to reduced dwell time | $988,000 | $988,000 | $988,000 | $2,964,000 | $2,457,010 |
| Ctr | Savings on third-party incident response services | $152,000 | $152,000 | $152,000 | $456,000 | $378,002 |
| Dtr | Cost savings from transition to the cloud | $131,220 | $131,220 | $131,220 | $393,660 | $326,325 |
| | Total benefits (risk-adjusted) | $1,501,450 | $1,501,450 | $1,501,450 | $4,504,350 | $3,733,885 |

### SECURITY TEAM EFFICIENCY GAINS

**Evidence and data.** After deploying Exabeam, the SOC could review and investigate security logs, alerts, and incidents through a centralized single view. Not only does this reduce false positives but it also speeds mean time-to-respond and -resolve.

The CISO at the electronics firm had to take calculated risks before deploying Exabeam. They explained: "I had a philosophy that we should ingest the complete universe [of data sources]. But just one of my SOC agents was getting about a thousand incidents a day. There was no way we could process to that level. We had to unenroll services and focus on just what we felt was truly critical for us to be able to listen to and respond to." Because of the efficiencies Exabeam provides, the interviewees were able to improve their coverage by ingesting additional data sources and increase the number of incidents they were able to investigate.

Interviewees provided excellent examples of how their teams became more effective:

- The IT security chief at the retail and manufacturing firm described two ways his team could increase their mean time to detect. First, he said: "We work under SLAs. We had a 90-minute SLA from when we saw a critical alert until we confirmed an incident or discarded it as a false positive. We reduced time spent analyzing by hand, no more going individually to the different consoles for the network, web servers, and antivirus, for example. Because of our use of Exabeam, we felt comfortable reducing our SLA from 90 to 45 minutes."

  Second, the IT security chief discussed the role process automation played in developing greater efficiency: "I'm a big believer in the MITRE ATT&CK framework, and I asked my team to map everything to it.[4] We developed scripts to input information from Exabeam. We built heatmaps and created a specific detection and coverage on four different use cases, alerts, and threats. We used all the models Exabeam includes and asked them to map back to the ATT&CK framework for each technique. In the end, we took that information and created automatic scripts, which helped with threat hunting."
- The CISO of the mining firm said: "The analytic engine takes log sources and correlates them together, assigns risk points for users and assets,

and we investigate when they hit a score of over 90 points. After investigating those incidents, we can do threat hunting inside the tool. We used to see up to 100 incidents a day, but the longer we use Exabeam, we've seen dramatic drops of about 70% to 75%. I would attribute nearly all of that decrease in the number of incidents to the fact that we have Exabeam running in our environment."

**"We're a global company. Even though we don't have a huge number of employees, the disparity of our networks is what makes our situation unique. We've noticed as we implemented our risk and vulnerability strategy, addressing the things the risk analysis tool was calling out, our risk scores have gone down dramatically in just a few months. Along with that comes a decrease in the number of incidents that we're dealing with daily. There is a direct correlation there."**

*CISO, mining*

- The CISO of the chemicals firm discussed how centralized monitoring allowed him to reduce the number of staff they needed: "There's reduced staff requirements because of centralized monitoring, and the alerting is excellent. I can do what I do with a couple of people, and once you get somebody up to speed, it's easy to train them to run the reports. I have an analyst who was an intern, and one of the first things we put him on was being able to do those views in Exabeam to monitor and alert the right people."
- The CISO of the mining firm said: "When we do need to investigate something, Exabeam eliminates hours of scouring through logs down to just a few minutes. If I see something that looks like a lateral movement, I hit the timeline in Exabeam and pull up log entries directly out of the Exabeam tool instead of writing correlation rules on a traditional SIEM or manually hunting through logs on your own. It's saved us hours and hours and is one of the reasons we can get away with only two security people in our company."
- The IT security chief of the retail and manufacturing firm discussed how Exabeam increased their time-to-value by including the core library of correlation rules: "If I had to do that manually, I would have to ask each security control vendor for their catalog for each of the events they log. I would need to map the technique for each one of the controls; then, I would have to do the correlation myself. Exabeam already included the correlation rules in their latest modules. It would have been a considerable feat for us to do that automation without the correlation that Exabeam included."

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

- Before Exabeam Fusion SIEM, 2,600 security incidents needed manual investigation and resolution.
- Due to a lack of resources, the composite organization only had resources to investigate 25% of the 2,600 incidents before deploying Exabeam.
- Before Fusion SIEM, it took 360 minutes to investigate an incident.

- After deploying Fusion SIEM, it took 5 minutes to investigate an incident.
- It took a total of 234,000 minutes each year to investigate and resolve all incidents, before Exabeam.
- After deploying Exabeam, the composite was able to investigate 75% of the 2,600 incidents.
- After deploying Exabeam, it only took 9,750 minutes to investigate 75% of the 2,600 incidents.
- Based on an annual savings of 3,738 hours, the security team was able to save nearly $288,000.

**Risks.** Organizations may realize results that differ from those presented in the financial model due to:

- The size and average salary of the SOC team.
- The number of incidents that the organization is handling.
- The average time SOC analysts spend on false positives and advanced investigations.

**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 $573,000.

**“The value that Exabeam brought was better initial triage of those events that allowed us to ignore less. I think I would say at least 50%, probably more. The goal was to catch what was truly important. We now filter out more of the low-level noise more effectively to identify the critical-level risks that need to be investigated.”**

*CISO, electronics*

| Security Team Efficiency Gains | | | | | |
|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Source** | **Year 1** | **Year 2** | **Year 3** |
| A1 | Annual number of security incidents that need manual investigation and resolution | Interview | 2,600 | 2,600 | 2,600 |
| A2 | Percent of incidents that were investigated before Exabeam | Interviews | 25% | 25% | 25% |
| A3 | Actual time to investigate and resolve an incidence before Exabeam(minutes) | Interviews | 360 | 360 | 360 |
| A4 | Actual time to investigate and resolve an incidence after Exabeam (minutes) | Interviews | 5 | 5 | 5 |
| A5 | Time (minutes) needed to investigate and resolve incidences, before Exabeam | Interviews | 234,000 | 234,000 | 234,000 |
| A6 | Percent of incidents that were actually investigated after Exabeam | Interviews | 75% | 75% | 75% |
| A7 | Time needed (in minutes) to investigate and resolve incidences after Exabeam | Interviews | 9,750 | 9,750 | 9,750 |
| A8 | Annual time savings (hours) | A5-A7/60 | 3,738 | 3,738 | 3,738 |
| A9 | Security analyst hourly compensation, fully burdened | TEI standard | $77 | $77 | $77 |
| At | Security team efficiency gains | A8*A9 | $287,788 | $287,788 | $287,788 |
| | Risk adjustment | ↓20% | | | |
| Atr | Security team efficiency gains (risk-adjusted) | | $230,230 | $230,230 | $230,230 |
| | **Three-year total: $690,690** | | **Three-year present value: $572,548** | | |

### DECREASED FINANCIAL EXPOSURE DUE TO REDUCED DWELL TIME

**Evidence and data.** Data theft requires access to the data. That access is either obtained by external actors who, using compromised credentials, masquerade as insiders, or granted to an insider as part of their job. Insiders can be any employee, contractor, partner, or vendor who has access to your firm's data and systems. Today, most security teams focus their security controls on external threats and fail to treat the insider threat as a major threat vector. Understanding user behavior is key for finding malicious insiders and compromised accounts. Damage from threats comes in several forms: fraud, intellectual property theft, sabotage and destruction, snooping, leaking, and doxing.[5]

Interviewees were well aware of the risks that these internal and external threats cause; however, many lacked the security infrastructure resources to recognize these threats before real value was stolen from their organizations. Two interviewees described scenarios where millions of dollars of intellectual property theft occurred. The CISO of the mining firm said: "We had an insider threat breach a couple of years ago where intellectual property data was stolen by a citizen of another country. No GDPR data was compromised, but intellectual property was. The cost to us could have been in the millions."

The CISO of the mining firm continued: "Prior to [deploying Exabeam], you might identify that something doesn't look quite right. You would go to firewall and active directory logs as well as other systems, combing through those for that person's name. You're probably already four or five hours in, without even starting any of the correlation work yet. Exabeam does that all for you with a few clicks get to

entire timeline of everything they've done throughout that day just simply coming from the log files. It literally takes five [or] six hours' worth of work down to a few minutes." He went on to describe that he could quickly further his investigation, which allowed him to contact the person to ask relevant questions: "You start seeing those correlations and making those decisions in a rather rapid manner. You've already seen all of that from the matter of just clicking on a popped-up alert inside of the tool that otherwise would have taken you five, six, seven, maybe even eight [hours], maybe even days' worth to figure out."

**"You can start asking relevant questions, calling a person to inquire why you saw them log in from Delhi, India, and then five minutes from Australia." We all know the answer to that is no. That's where you start seeing correlations and making decisions in a rapid manner. You see that from just clicking on a popped-up alert inside of the tool that otherwise would have taken you five, six, seven, maybe even days' of time to figure out."**

*CISO, mining*

The CISO of the chemicals company described their risk-based approach to investigations: "You always want to see all the movement in your security system. You want to know when admins are logging into executive PCs. We track high-risk systems and have specific alerts set to track executives, because many times they're targeted. Most systems can see that somebody logging into a system, but in Exabeam, we can see that the system is an executive, and it's an admin logging in. Admins have superior privileges, but it could look like a hacker that's broken into the system and accessing an executive system. Because we can see those details, it helps you identify and fix problems quicker."

The IT security chief at the retail and manufacturing firm experienced a scenario where there were attacks against financial transactions. Prior to deploying Exabeam, they didn't have visibility into these transactions. This incident drove the need to expand their monitoring of user behavior to cover more critical infrastructure. They said: "With Exabeam, I can do behavior. I can do some things that are very advanced compared to doing just static rules on a SIEM."

The IT security chief described how Exabeam impacted their dwell time: "The last incident we handled, Exabeam and our other tools helped us cut our dwell time. We went from days to minutes. In just minutes, we detected him but watched each of his actions for 10 more minutes to confirm before kicking him out of the server. Previously, it took us up to 48 hours being inside the server before we noticed something was happening because he had to try to do something outside of the server or move laterally or do something else in the kill chain. Now, we detected him as soon as he touched the server because we had good visibility in all those critical servers. Exabeam gives us that quick alert and quick possibility to do the incident response with the incident response module [and] to use the SOAR to do orchestration and automation on some of the things we're seeing."

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

- Based on the losses described in the interviews, the composite organization experienced losses of $2 million each year.

- "Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020" revealed that 65% of companies with between 20,000 and 50,000 employees experienced a breach every year.
- Interviewees were able to reduce their dwell time by 95% — from months to minutes.

**Risks.** Risks that may impact financial exposure due to reduced dwell time include:

- The number of breaches the organization experiences each year.
- The financial impact of each breach.
- The ability of the security team to react to Exabeam's alerts.

**Results.** To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $2.5 million.

**Decreased Financial Exposure Due To Reduced Dwell Time**

| Ref. | Metric | Source | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|
| B1 | Cost of Stolen IP | Interview | $2,000,000 | $2,000,000 | $2,000,000 |
| B2 | Probability of an incident occurring | Forrester custom research | 65% | 65% | 65% |
| B3 | Decrease in vulnerability window from using Exabeam | interview | 95% | 95% | 95% |
| Bt | Decreased financial exposure due to reduced dwell time | B1*B2*B3 | $1,235,000 | $1,235,000 | $1,235,000 |
| | Risk adjustment | ↓20% | | | |
| Btr | Decreased financial exposure due to reduced dwell time (risk-adjusted) | | $988,000 | $988,000 | $988,000 |
| | **Three-year total: $2,964,000** | | | **Three-year present value: $2,457,010** | |

### SAVINGS ON THIRD-PARTY INCIDENT RESPONSE SERVICES

**Evidence and data.** Cybersecurity incident response service providers offer critical support during cybersecurity breaches. They provide incident response and digital forensics expertise on demand to support customers hit by cybersecurity attacks such as data breaches, malware outbreaks, and ransomware infections that disrupt operations.[6]

The CISO at an electronics firm described how Exabeam not only helped them save money previously spent with cybersecurity incident response services providers but also helped them feel confident in their legal defense preparation.

The electronics firm CISO explained: "We had been down the path of forensics and evidence collection and made a specific decision to contract with a certified third-party to perform those collections for us. The main reason that we wanted to do that was we didn't have any certified forensic experts on our team. If they were deposed, they are in a weaker position that wouldn't be helpful to our case, so we outsource completely. Now, to collect defense data, we pull from Exabeam as one of the sources or collection points. It costs hundreds of thousands of dollars to hire a third party, depending on the size of the collection and the amount of time. There was one event that was over $100,000 in just the investigation component, not even other legal aspects."

**Modeling and assumptions.** Based on customer interviews, Forrester estimates that the composite organization spends $200,000 on a yearly basis with cybersecurity incident response services providers. Using Exabeam, the composite was able to reduce their spend with third party providers by 95%.

**Risks.** The savings on third-party services will vary with:

- The number of security incidents that require forensic investigation.
- The size of the firm previously hired and the scope of services they were contracted to perform.

**Results.** To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $378,002.

**Savings On Third-Party Incident Response Services**

| Ref. | Metric | Source | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|
| C1 | Dollars previously spent on forensic collection | Composite | $200,000 | $200,000 | $200,000 |
| C2 | Decrease in vulnerability window from using Exabeam (From months to minutes) | interview | 95% | 95% | 95% |
| Ct | Savings on third-party incident response services | C1*C2 | $190,000 | $190,000 | $190,000 |
| | Risk adjustment | ↓20% | | | |
| Ctr | Savings on third-party incident response services (risk-adjusted) | | $152,000 | $152,000 | $152,000 |
| | **Three-year total: $456,000** | | | **Three-year present value: $378,002** | |

### COST SAVINGS FROM TRANSITION TO THE CLOUD

**Evidence and data.** Legacy on-premises solutions suffered from storage capacity and compute limitations that are minimized in the cloud. Cloud-hosted solutions are easier to manage and maintain than on-premises hardware or software, helping with scalability and offloading maintenance to the provider.[7] Interviewees had different reasons for selecting a cloud-based provider. Still, all resulted in value for their companies.

- For the CISO at the retail and manufacturing firm, it was less about storage and more about the network. They explained: “In general, my philosophy is cloud-first. If I were considering building an on-premises SIEM, I’m not sure it would be on-premises. It would probably be in [a

**“The biggest thing I saw with on-prem SIEMs is capacity management. To run a query against three years’ worth of logs bogs down the system. When you get multiple queries that are running against these infrastructure components, you’re hamstrung by their capabilities. Exabeam does a better job of scaling that performance.”**

*Head of global operations, financial services*

cloud services provider] because traditional data centers are dying."

- For the CISO at the chemicals firm, the advantage for moving their SIEM to the cloud was about the reduced cost of system management. He explained: "The cost savings were that we didn't have to handle our equipment; we didn't have to patch the equipment. We didn't have to upgrade it and maintain it, which took a fourth of a person, so that's a big cost saving." In addition, he also described benefits from reduced downtime: "In the past, we'd be down for a couple of days sometimes, and while the entire system wouldn't be down, we might lose some functionality built into the system. Now, because of redundancy built into the cloud, it's been three and a half years we are hardly down. Cloud is the way to go."

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

- The organization shuts down its four on-premises servers in the first year it implements Exabeam Fusion SIEM.
- The organization reassigns one IT FTE from server/network-related infrastructure management to value-add projects.

**Risks.** Cost savings from the transition to the cloud may vary depending on the following:

- The cost of the hardware previously used for the former on-premises security system(s).
- The costs of software, maintenance, and facilities.
- IT or security staff dedicated to security-related infrastructure management.

**Results.** To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $326,000.

**"Software as a service has taken over the industry for the last 10 years. Why not security? Especially considering the economies of scale you get with data linking. Regulators require us to carry significant log data for three years. To do that, you've got to buy servers, expand storage, and then maintain it all. I have the alternative of giving this data to Exabeam to manage. I understand the pitfalls of large data storage that goes away when you put that burden on Exabeam to manage it. The caveat is they have to be good at it!"**

*Head of global operations, financial services*

| Cost Savings From Transition To The Cloud | | | | | |
|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Source** | **Year 1** | **Year 2** | **Year 3** |
| D1 | Servers avoided due to moving to the cloud | Interviews | 4 | 4 | 4 |
| D2 | Server cost | Industry average | $5,000 | $5,000 | $5,000 |
| D3 | Network cost per server | Industry average | $750 | $750 | $750 |
| D4 | Server/network hardware maintenance | Industry average | $4,500 | $4,500 | $4,500 |
| D5 | Software costs | Industry average | $2,500 | $2,500 | $2,500 |
| D6 | Server software maintenance | Industry average | $1,500 | $1,500 | $1,500 |
| D7 | Server/network power, cooling, and facilities | Industry average | $7,200 | $7,200 | $7,200 |
| D8 | Infrastructure costs saved | D1*(D2+D3+D4+D5+D6+D7) | $85,800 | $85,800 | $85,800 |
| D9 | Number of IT FTEs managing the infrastructure for on-premises solution | Interviews | 1 | 1 | 1 |
| D10 | Percent of IT FTE's time dedicated to server/network management | Assumption | 50% | 50% | 50% |
| D11 | IT FTE fully burdened annual salary | TEI standard | $120,000 | $120,000 | $120,000 |
| D12 | Subtotal: reduction in server/network admin costs | D9*D10*D11 | $60,000 | $60,000 | $60,000 |
| Dt | Cost savings from transition to the cloud | D8+D12 | $145,800 | $145,800 | $145,800 |
| | Risk adjustment | ↓10% | | | |
| Dtr | Cost savings from transition to the cloud (risk-adjusted) | | $131,220 | $131,220 | $131,220 |
| | **Three-year total: $393,660** | | | **Three-year present value: $326,325** | |

### UNQUANTIFIED BENEFITS

Additional benefits that customers experienced but were not able to quantify include:

- **Reduced SLA to the business.** Leveraging Exabeam gave the IT security chief at the retail and manufacturing firm the confidence to guarantee shorter response times to business partners. They said: “The investigation time to confirm an alert was greatly reduced. I was able to decrease my SLA from 90 to 45 minutes.”
- **Faster time-to-value.** The regional CISO at a holding company noted: “It allows time-to-market. There are a lot of companies out there that have significant security deficiencies, and it looks extremely overwhelming to face them. You have to get a good control of your infrastructure for you to get control of your security. It gives us significant flexibility where we don’t have to rely on any outside teams.”
- **Infrastructure team benefits.** The CISO of the chemicals firm discussed how the infrastructure team uses Exabeam. “If someone is having trouble connecting, IT needs to see certain logs across networking devices or firewalls to understand why traffic is blocked. We have an

implementation of SaaS applications. If somebody can't get into those applications, we log those. They use it every day. They use it as much as we do. It's good information for everybody."

**"Exabeam's UEBA stack — and I've talked to all the product developers [at Exabeam] — is the best in the business. What they do for behavior analytics is fantastic."**

*CISO, retail and manufacturing*

- **Management-level visibility.** The CISO of the chemicals firm uses the metrics captured in Exabeam to stay ahead of important changes they're seeing in their ecosystem. The said: "As the CISO, I can see changes that are important to me. For example, I see that the number of vulnerabilities has gone up in one location. It gives me the ability to say, 'What's going on at that location? We need to get out there and check things out,' or 'Are they missing patches?' I don't know if I can't quantify that in terms of time and money, but it gives me and executive management a view into our important metrics. I don't know that I can put a dollar value on it, but it's definitely saving us money."
- **Eased staffing challenges.** The CISO of the electronics firm said, "We were able to operate effectively with the less-skilled resource." The regional CISO of the holding company concurred: "I am not afraid of a tier 1 person leaving the company because the tools do the job for them and the ramp-up time for them to become effective on the team is very fast. I don't worry about a revolving door at the tier 1 level." He described how he would offer opportunities to employees from IT, for example, who had the characteristics required to be a solid security performer: "I hired someone who had been in IT for a long time and wanted to try something else. He had never done cybersecurity in his life, [but he] did things to help enable it, such as documenting better cybersecurity practices. We ramped that person up in three months, and his manager said, 'He is the fastest ramp-up and the best hire I've ever had. A lot of that is the person's will, but it's also having the right tools. It's not just Exabeam, to be fair, but Exabeam is a great part of it.'"

**FLEXIBILITY**

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

- **Expanded visibility into integrated security tools.** The head of global operations at the financial services firm said: "We just purchased a threat intelligence platform that we've integrated in Exabeam. We're starting to focus on the threat intel journey and the indicators of compromise (IOCs). The fact that Exabeam integrates with several threat intelligence products is super important. I'm a firm believer in TIPs [threat intelligence platforms]. We use [another] threat intelligence platform, and then I pull in the feeds where I feel we need to get feeds from. I think that's a very reliable methodology for managing threats."
- **Improved tracking of metrics.** Prior to Exabeam, all the interviewees struggled to answer questions specifically related to metrics such as mean time-to-detect or mean time-to-repair. One electronics industry CISO revealed how they will leverage Exabeam now to track these valuable metrics: "Because of the volume of incidents coming in, the team could only keep

up with processing them based on their significance to the business. That is something that we aspire to do here. We haven't done that yet primarily because we didn't have the tools to do it. Security is one of those things that people will share a little bit but never the whole picture."

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

**"Prior to having this tool and others, I wouldn't even know where to start for IOCs. You get so wrapped up in trying to figure out where it came from, but you're not even thinking about tearing that piece of network apart and finding out what the indicators are compromised for and then threat-hunting the rest of your organization for those. If you don't have a tool in place to do that, you might as well just not even try."**

*CISO, mining*

# 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** |
| Etr | Annual fees paid to Exabeam | $0 | $345,000 | $345,000 | $345,000 | $1,035,000 | $857,964 |
| Ftr | Implementation and training | $98,640 | $81,816 | $32,256 | $32,256 | $244,968 | $223,910 |
| | Total costs (risk-adjusted) | $98,640 | $426,816 | $377,256 | $377,256 | $1,279,968 | $1,081,874 |

### ANNUAL FEES PAID TO EXABEAM

**Evidence and data.** The interviewees' organizations paid annual fees for the use of Exabeam Fusion SIEM as well as an additional fee to use Exabeam's Premier Success Plan technical support.

**Modeling and assumptions.** For the composite organization, Forrester assumes:

- The composite organization pays a total of $250,000 in annual fees to Exabeam.
- An additional 15% of total net fees is paid to Exabeam to cover the Premier Success Plan.

**Risks.** Costs may vary among organizations according to the following factors:

- Number of gigabytes ingested per day.
- Whether or not organizations opt for the cloud archive add-on for Fusion SIEM.
- The number of seats covered for the Exabeam Fusion Enterprise edition Incident Responder add-on.
- Whether or not organizations opt for the Exabeam Premier Success Plan.

**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 $857,964.

| Annual Fees Paid To Exabeam | | | | | | |
|---|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Source** | **Initial** | **Year 1** | **Year 2** | **Year 3** |
| E1 | Fees paid to Exabeam | Composite | | $250,000 | $250,000 | $250,000 |
| E2 | Premier Success Plan fees | 15%*E1 | | $37,500 | $37,500 | $37,500 |
| Et | Annual fees paid to Exabeam | E1+E2 | $0 | $287,500 | $287,500 | $287,500 |
| | Risk adjustment | ↑20% | | | | |
| Etr | Annual fees paid to Exabeam (risk-adjusted) | | $0 | $345,000 | $345,000 | $345,000 |
| | **Three-year total: $1,035,000** | | | **Three-year present value: $857,964** | | |

### IMPLEMENTATION AND TRAINING

**Evidence and data.** The interviewed decision-makers told Forrester that implementation costs were both internal and external in nature, with fees paid to Exabeam and a few weeks of internal effort both contributing to overall costs.

- The interviewees also told Forrester that they paid Exabeam an initial training fee.
- Additional internal effort was required over the investment for both training and ongoing maintenance of the platform.

**"Exabeam does a very good job of holding your hand during implementation. They're with you every step of the way."**

*CISO, mining*

**Modeling and assumptions.** For the composite organization, Forrester assumes:

- An initial fee of $75,000 paid to Exabeam for implementation.
- An additional fee of $24,500 paid to Exabeam for training in the first year of the investment.
- Two analysts working at half-time for three weeks are required for implementation.
- Eight security analyst team members undergo five days of training in Year 1, decreasing to one analyst in Years 2 and 3.
- One analyst spends 20% of their time on maintenance.

**Risks.** Costs may vary among organizations according to the following factors:

- Size and type of fees paid to Exabeam.
- Number and type of employees needed for implementation.
- Number and type of employees needed for training.
- Number and type of employees needed for ongoing maintenance.
- Total amount of time to implement Exabeam and train employees.

**Results.** To account for these risks, Forrester adjusted this cost upward by 20%, yielding a three-year, risk-adjusted total PV of $233,910.

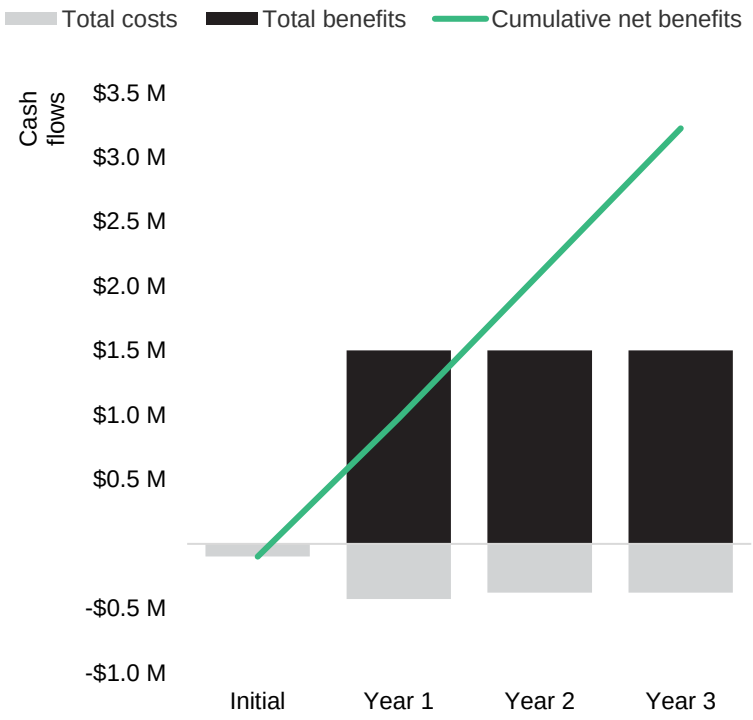
## Implementation And Training

| Ref. | Metric | Source | Initial | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|---|
| F1 | Implementation fees paid to Exabeam | Exabeam | $75,000 | | | |
| F2 | Time spent on implementation (hours) | Composite | 120 | | | |
| F3 | Analysts needed for implementation | Composite | 2 | | | |
| F4 | Average analyst fully burdened hourly salary | TEI standard | $60 | $60 | $60 | $60 |
| F5 | Analyst time needed for implementation | Composite | 50% | | | |
| F6 | Subtotal: implementation costs | F1+(F2*F3*F4*F5) | $82,200 | | | |
| F7 | Fees paid to Exabeam for training | Exabeam | | $24,500 | | |
| F8 | Security analysts | Composite | | 8 | 1 | 1 |
| F9 | Security analyst training time (hours) | Composite | | 40 | 40 | 40 |
| F10 | Subtotal: training cost | F8*F9*F4 | | $19,200 | $2,400 | $2,400 |
| F11 | Analysts needed for ongoing maintenance | Interviews | | 1 | 1 | 1 |
| F12 | Percentage of analyst's time for ongoing maintenance | Interviews | | 20% | 20% | 20% |
| F13 | Subtotal: ongoing maintenance cost | (F4*2040)*F11*F12 | | $24,480 | $24,480 | $24,480 |
| Ft | Implementation and training | F6+F10+F13 | $82,200 | $68,180 | $26,880 | $26,880 |
| | Risk adjustment | ↑20% | | | | |
| Ftr | Implementation and training (risk-adjusted) | | $98,640 | $81,816 | $32,256 | $32,256 |
| | **Three-year total: $244,968** | | | **Three-year present value: $223,910** | | |

# 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 | ($98,640) | ($426,816) | ($377,256) | ($377,256) | ($1,279,968) | ($1,081,874) |
| Total benefits | $0 | $1,501,450 | $1,501,450 | $1,501,450 | $4,504,350 | $3,733,885 |
| Net benefits | ($98,640) | $1,074,634 | $1,124,194 | $1,124,194 | $3,224,382 | $2,652,011 |
| ROI | | | | | | 245% |
| 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: Endnotes

[1] Source: “Defend Your Digital Business From Advanced Cyberattacks Using Forrester’s Zero Trust Model,” Forrester Research, Inc., June 25, 2021.

[2] Source: Charlie Osborne, “The more cybersecurity tools an enterprise deploys, the less effective their defense is,” ZDnet, June 30, 2020 (https://www.zdnet.com/article/the-more-cybersecurity-tools-an-enterprise-deploys-the-less-effective-their-defense-is/).

[3] 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.

[4] MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. Source: The MITRE Corporation (https://attack.mitre.org/).

[5] Source: “Best Practices: Mitigating Insider Threat,” Forrester Research, Inc., March 18, 2021.

[6] Source: “Now Tech: Cybersecurity Incident Response Services, Q4 2021,” Forrester Research, Inc., December 2, 2021.

[7] Source: “Adapt Or Die: XDR Is On A Collision Course With SIEM And SOAR,” Forrester Research, Inc., April 28, 2021.


FORRESTER®