FORRESTER®

The Total Economic Impact™ Of DTEX

Business Benefits Enabled By DTEX

January 2025

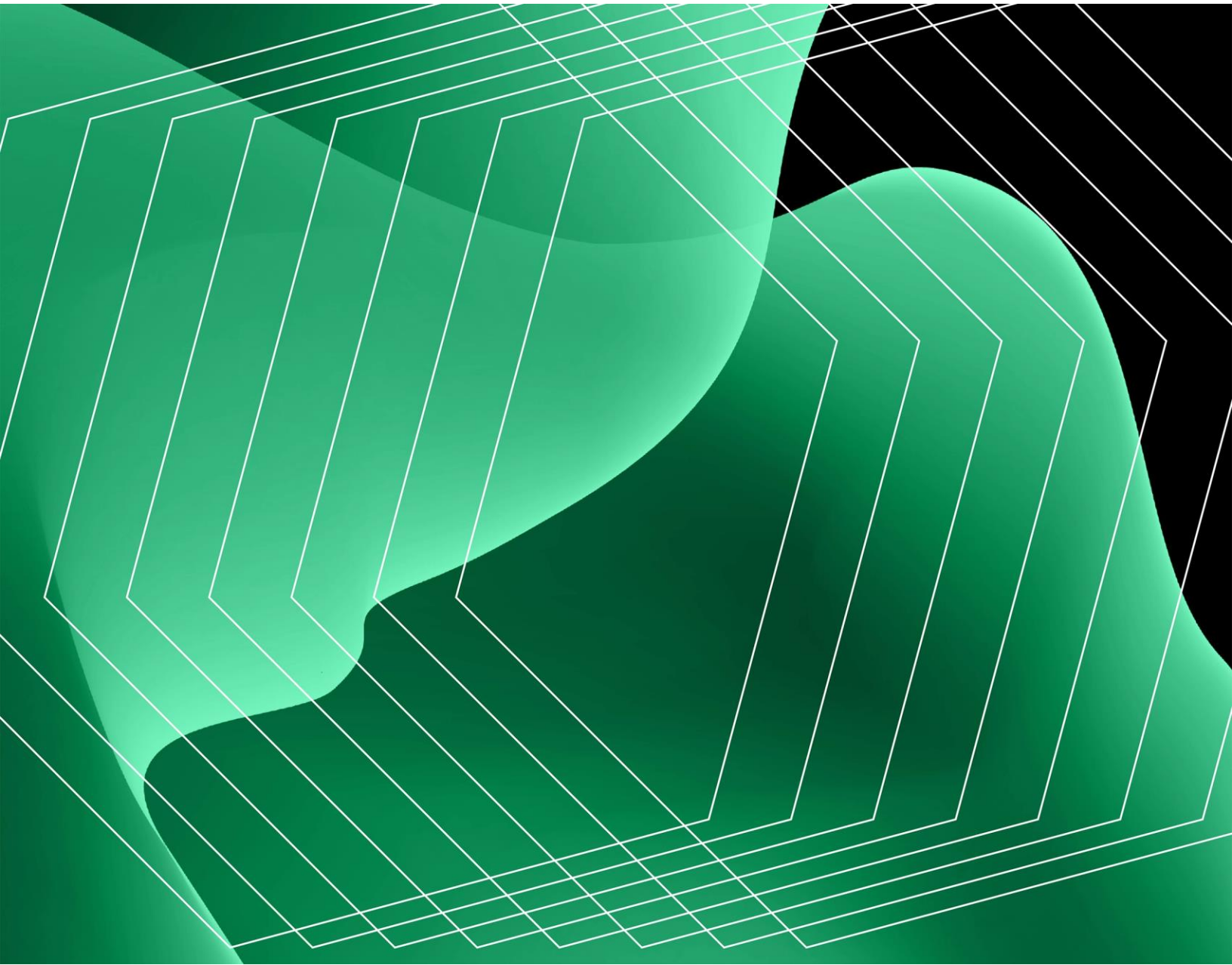

Table Of Contents

Consulting Team:

Nikoletta Stergiou

Luca Son

ABOUT FORRESTER CONSULTING

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

Executive Summary

Although insider incidents comprise a large percentage of data breaches, many security teams don't prioritize insiders as a threat vector and instead focus their efforts almost exclusively on external threats.[1] Security teams need a tool that can provide a comprehensive view of user behavior across their entire organization, allowing them to proactively detect and address potential risks from within — including those from compromised credentials.

DTEX provides advanced insider threat detection and risk management solutions that continuously monitor and analyze user behavior and activities. Using sophisticated analytics and real-time data to identify the intent behind user behavior, DTEX enables organizations to mitigate potential security threats by proactively identifying risky behavior across an enterprise before they escalate. It also consolidates data loss prevention (DLP), user entity and behavior analytics (UEBA), and user activity monitoring (UAM) to foster a culture of security and trust. This comprehensive approach helps protect sensitive information and stop data loss through dynamic risk scoring. DTEX boosts security operation center (SOC) activities with behavioral intelligence and accelerates incident response with real-time forensics.

DTEX commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential benefits and financial impacts enterprises may realize by deploying DTEX.[2]

To better understand the benefits and risks associated with this investment, Forrester interviewed five representatives with experience using DTEX. The representatives work at organizations in telecommunications, pharmaceuticals, banking, and energy industries that range from 8,000 to 150,000 employees. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a multibillion-dollar North American-based global enterprise in the critical infrastructure space with 50,000 employees and 30,000 endpoints monitored by DTEX.

Interviewees said that prior to using DTEX, their organizations had disparate tooling and limited capabilities to stand up a comprehensive insider risk program. Prior environments did not provide adequate visibility into user behavior and insider risk, creating difficulty in identifying and stopping data leaks, account misuse, AI abuse, intellectual property (IP) theft, co-employment, and more. Previous efforts to address incidents were reactive, manual, and piecemeal.

After the investment in DTEX, the interviewees noted that they enhanced data security, gained visibility into all data movement (including file name changes), and captured a comprehensive picture of user behavior. Interviewees said that these updates enabled them to reduce their security stack and total cost of ownership (TCO), increase operational efficiency, and improve regulatory compliance, which ultimately led to reduced risk of costly insider data breaches and improved overall organizational resilience.

KEY FINDINGS

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

- **Tech stack consolidation worth $3.3 million over three years.** The composite organization decreases its TCO by consolidating multiple security functions into a single, integrated platform, allowing it to retire costly legacy solutions. By combining user behavior analytics, user monitoring, and forensics into one cohesive system with DTEX, the composite can eliminate the need for disparate tools and associated management and maintenance expenses. This consolidation not only reduces software and hardware costs but also minimizes the administrative burden on IT teams, leading to lower operational expenses.
- **Insider risk efficiencies worth $705,000 over three years.** The composite organization enhances insider risk analyst productivity by gaining comprehensive, real-time visibility into user activities, thereby reducing the time required for investigations. Using DTEX, analysts can focus on user behavior and activities by continuously monitoring applications to spot suspicious events with full context. This streamlined approach not only accelerates the investigation process but also enhances threat detection accuracy, enabling analysts to focus on high-value tasks such as risk mitigation and strategy development.

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

- **Avoided data breach costs.** By continuously assessing user behavior and context, DTEX helps the composite identify insider threats, compromised accounts, and data exfiltration attempts with higher precision than was possible in the prior environment.

This proactive approach ensures that security teams are promptly alerted to suspicious activities, enabling them to take quick and effective action to mitigate risks.

- **Protected IP.** The composite can increase its IP protection with DTEX, including AI initiatives, by constantly monitoring and analyzing user behavior, detecting potential insider threats, preventing data loss through policy enforcement, and facilitating efficient incident response.
- **Improved policy configuration and management.** The composite streamlines its policy configuration and management using DTEX's out-of-the-box, customizable policies.
- **Improved collaboration between security and other teams.** Insider risk spans cross-functional groups: legal teams are often tasked with providing compliance guidance and HR assists in recognizing insider risks. With DTEX, the composite strengthens its cross-functional collaboration and threat management efforts across cybersecurity, legal, HR, IT, and other related teams.
- **Reduced shadow IT.** DTEX helps the composite organization detect shadow IT by collecting and analyzing information on devices, applications, and users. This enables security teams to safeguard non-IT systems from internal and external malicious attacks, enhancing overall cybersecurity.

The representative interviews and financial analysis found that a composite organization experiences quantified benefits of $3.99 million over three years. There are also several unquantified benefits that could add value to organizations.

75%

Reduction in investigation time with DTEX

> “No one can deny the benefit that DTEX has provided. … The return on investment that we’ve been able to get from the tool has been great.”
>
> MANAGER OF GLOBAL CYBER DETECTION AND RESPONSE, TECHNOLOGY

> “DTEX has provided rich context of worker behavior that has allowed us to more accurately determine intent and respond to events that we would not have previously seen. Our use case customizations allow us to pivot to any situation we are concerned about.”
>
> DIRECTOR OF INSIDER RISK, PHARMACEUTICALS

Quantified Benefits PV

$3.99M

Reduction in investigation time with DTEX

75%

Tech stack consolidation savings

$3.29M

Benefits (Three-Year)

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in DTEX.

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

DISCLOSURES

Readers should be aware of the following:

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

Forrester makes no assumptions as to the potential benefits 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 using DTEX.

DTEX 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.

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

Due Diligence
Interviewed DTEX stakeholders and Forrester analysts to gather data relative to DTEX.

Interviews
Interviewed five representatives at organizations using DTEX to obtain data about 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 interviewees.

Case Study
Employed fundamental elements of TEI in modeling the investment impact: benefits, flexibility, and risks. Given the increasing sophistication of financial 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.

Customer Journey

Drivers leading to the use of DTEX

Interviews				
Role	**Industry**	**Region**	**Revenue**	**Total Endpoints**
Senior director of the threat management center	Telecommunications	HQ in US, global operations	$134 billion	150,000
Director of insider risk	Pharmaceuticals	HQ in US, global operations	$54 billion	90,000
VP of cybersecurity	Banking	HQ in US, global operations	$36 billion	60,000
Senior manager of threat intelligence	Energy	HQ in US	$29 billion	53,000
Manager of global cyber detection and response	Technology	HQ in US, global operations	$3 billion	8,000 to 9,000

KEY CHALLENGES

Before DTEX, interviewees' organizations struggled to set up effective insider risk programs, thwarted by disparate tooling and limited capabilities. Prior environments, which included different DLP products, UEBA add-ons, and UAM products, provided inadequate visibility and context into user behavior, making it difficult to identify and investigate insider threat incidents. Efforts to prevent and address incidents were reactive, manual, and piecemeal. The interviewees noted how their organization struggled with common challenges, including:

- **Limited context in a complex tech stack.** Interviewees told Forrester that their security technology was challenging to manage, especially coming from multiple point solutions. Technology owners struggled to consolidate multiple security solutions while also managing potential gaps in their security posture. Insider threat workflows were siloed, leading to manual processes. The senior director of the threat management center at a telecommunications organization said, "Before DTEX, we were very siloed in the sense

that we had individual DLP alerts that would trigger, and then analysts would do a lot of manual correlation or manual searching and correlation to put the pieces together."

- **Delayed insights.** Interviewees said their environment before DTEX lacked visibility to identify and contextualize insider threats. Insider risk analysts struggled to investigate user activities and behavior within their networks and systems, putting them in a reactive state. The VP of cybersecurity at a banking organization told Forrester: "DTEX is a context tool — that is the best way to describe it. DTEX provides a holistic picture of user behavior such as, 'What were their activities before? What are their activities on their endpoint?' DTEX just gives us that visibility into things we didn't have before."

  The VP of cybersecurity continued: "Finding things that we didn't know about in our DLP content was impossible. We didn't have the right technology in place — that was the single biggest challenge. With that comes, as I mentioned, being unable to correlate and unable to get to a predictive state. Everything is very reactive."
- **Limited resources.** Like many cybersecurity teams, interviewees faced difficulty hiring and retaining skilled cybersecurity personnel. As such, interviewees sought a solution to streamline insider risk workflows so they could spend their time on more strategic areas. The VP of cybersecurity at a banking organization said: "[Our prior solution] could not meet the basic DLP-type use case such as a basic email data exfiltration. We gave multiple chances to the solution vendor to follow our standard process when an employee was terminated. This included integrating with our [enterprise software] to look at users 60 days before termination and 60 days after to identify any data exfiltration. However, we struggled for an entire year to get them to do that basic case."
- **Prolonged exposure to potential damages.** Interviewees were left vulnerable to potential damages from insider threat incidents in their prior environment. They cited alert fatigue, lack of visibility, reactive approaches, and lengthy incident containment and resolution times as key issues which left their organization at risk of data exfiltration and security data breaches. The VP of cybersecurity at a banking organization said: "We basically had escalated the program because we had a bad thing happen. A person left the company and took one of our most confidential documents with them, and that escalated everything. This was the use case that we needed from a UEBA tool, but we were not able to get it done [in our prior environment]."

> "[Before DTEX], the ability to track an event that happened three months ago to a person was very difficult, to the point where we had thousands of keywords and a dictionary. We got very good at finding what we knew about but correlating information was much harder and finding things that we didn't know about in our DLP was impossible. … That was the single biggest challenge — not being able to correlate and get into a predictive state."
>
> DIRECTOR OF INSIDER RISK, PHARMACEUTICALS

SOLUTION REQUIREMENTS

Interviewees' organizations required a comprehensive insider risk management solution that could proactively identify and mitigate insider threats while maintaining employee privacy and network performance. As such, interviewees searched for a solution that could:

- Scale to monitor hundreds of thousands or even millions of endpoints.
- Collect and anonymize structured metadata to protect individual user identities using a privacy-centric approach.
- Manage insider threats through a comprehensive, consolidated platform that combines DLP, UAEM, and UAM capabilities.
- Manage risk proactively with early warning indicators and actionable insights to course-correct before incidents occur.
- Assign levels of risk to users and detect active insider threats using predictive analytics.
- Enable investigators to detect and respond to insider threats more effectively through enhanced visibility into user activities and behaviors with context and AI-guide investigations.

> “We went with a cloud solution, so we didn’t have to buy any of our own hardware or equipment or anything like that. Not having to purchase anything on-prem and being able to retain the data from the cloud was extremely valuable.”
>
> DIRECTOR OF INSIDER RISK, PHARMACEUTICALS

> “[DTEX] is both an enabler of business and a risk reducer of business, and that is why we have it.”
>
> VP OF CYBERSECURITY, BANKING

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and a benefits analysis that illustrates the areas financially affected. The composite organization is representative of the five 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 is a large US-based enterprise with global operations. The organization generates $30 billion in annual revenue, has 50,000 employees, and is a leader in the critical infrastructure space.

Deployment characteristics. The composite organization implements DTEX to consolidate its DLP, UEBA, and UAM point solutions to specifically address use cases like data loss (including exfiltration, data deletion, and fraud), account misuse, account compromise, AI misuse and abuse, flight risk, and co-employment. The composite organization replaces two legacy point

solutions with DTEX over three years. There are five insider risk analyst FTEs who cover 50% of the total 30,000 end points within the composite organizations networks and systems.

Key assumptions

$30 billion in annual revenue

50,000 employees

Five insider risk analysts

30,000 endpoints covered by DTEX

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	Tech stack consolidation	$900,000	$1,350,000	$1,800,000	$4,050,000	$3,286,251
Btr	Insider threat risk efficiencies	$283,500	$283,500	$283,500	$850,500	$705,023
	Total benefits (risk-adjusted)	$1,183,500	$1,633,500	$2,083,500	$4,900,500	$3,991,274

TECH STACK CONSOLIDATION

Evidence and data. DTEX helped interviewees' organizations decrease their TCO by consolidating multiple security functions into a single, integrated platform, which allowed them to retire costly legacy solutions. By combining user behavior analytics, user monitoring, and forensics into one cohesive system, interviewees noted that DTEX eliminated the need for disparate tools and associated management and maintenance expenses. This consolidation not only reduced their software and hardware costs but also minimized the administrative burden on IT teams, leading to lower operational expenses.

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

- The composite organization leverages two point solutions before DTEX, each costing an average of $1 million annually.
- The composite organization sunsets one of these point solutions in Year 1 and has sunset both solutions by Year 3.

Risks. Forrester recognizes that these results may not be representative of all experiences. The impact of this benefit will vary depending on:

- The number, size, and breadth of prior insider risk solutions.
- The technological complexity and ongoing management requirements.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $3.3 million.

> "We were able to get rid of our DLP solution as we were really focused on detective capabilities with DTEX, so there was a million dollars of savings there."
>
> VP OF CYBERSECURITY, BANKING

Tech Stack Consolidation					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Retired point solutions	Interviews	1	1.5	2
A2	Average annual cost per point solution	Interviews	$1,000,000	$1,000,000	$1,000,000
At	Tech stack consolidation	B1*B2	$1,000,000	$1,500,000	$2,000,000
	Risk adjustment	↓10%			
Atr	Tech stack consolidation (risk-adjusted)		$900,000	$1,350,000	$1,800,000
	Three-year total: $4,050,000			**Three-year present value: $3,286,251**	

INSIDER THREAT RISK EFFICIENCIES

Evidence and data. Interviewees told Forrester that DTEX enhanced the productivity of insider risk analysts by providing comprehensive, real-time visibility into user activities, thereby reducing the time required for investigations. DTEX's analytics and behavior-based threat detection allowed analysts to quickly identify and prioritize genuine risks and reduce false

positives, eliminating the need to manually sift through vast amounts of data. This streamlined approach not only accelerates the investigation process but also enhances threat detection accuracy, enabling analysts to focus on high-value tasks such as risk mitigation and strategy development. DTEX's reporting and dashboards also helped simplify workflow management, further improving operational efficiency and allowing teams to proactively address potential threats before they escalated.

Additionally, interviewees highlighted the impact of DTEX's Ai^3 Risk Assistant on investigator efficiencies. The Ai^3 Risk Assistant helped interviewees proactively identify malicious intent by uncovering where sensitive data was being stored and how and why it was being transferred. Interviewees provided the following evidence:

- The senior manager of threat intelligence noted their energy organization cut insider risk investigation time by half. The interviewee said, "For a case that would traditionally take one investigator 40 hours to run down, we've been able to probably cut that time in half, especially if the DTEX agent is on the endpoint."

  Insider risk analysts at this interviewee's organization also saved time configuring policies. The senior manager of threat intelligence continued: "Normally, trying to seek out [our security information and event management (SIEM)] and guessing the next tool was a manual process. With DTEX, the custom policies and even the out-of-the-box policies in the toolset have allowed us to save time and resources from that manual hunt and it helps identify it right there."

  The director of insider risk at a pharmaceutical organization said: "We've been able to take 50% of one person's time and move it from DLP to insider risk with DTEX. And then we've been able to take 25% from three other people that would have also been working 100% on DLP."

  The senior director of the threat management center at a telecommunications organization told Forrester: "I would say it's a matter of spending 10 to 15 minutes with DTEX as opposed to potentially 2 or 3 hours pivoting into multiple systems, pulling the logs, and correlating information in a spreadsheet."

Beyond time savings, DTEX helped interviewees increase their accuracy and confidence:

- The director of insider risk at a pharmaceutical organization said: “DTEX helps us correlate events to gain a higher confidence factor in the event. We have created custom use cases, such as steganography, whereas those events would have been previously unavailable. We are also seeing local device activities when users are not connected to the corporate network that we previously would not have seen.”

  The VP of cybersecurity at a banking organization explained: “DTEX enables [investigators] to do more investigations, but also more thorough investigations, faster. Especially when we have junior investigators, they don’t want to get it wrong. You’re talking about a person’s livelihood, so having a tool that you can rely on to provide a clear, holistic view gives them confidence. DTEX gives them a high level of confidence and enables them to move on to their next investigation faster.”

> “We’re taking advantage of the i3 services that DTEX offers. They help us fine-tune our alerts with context. For example, this group of users is in the finance department, so their normal activity is going to be very different to another group. Having that additional layer is a huge help in reducing or increasing the activity.”
>
> MANAGER OF GLOBAL CYBER DETECTION AND RESPONSE, TECHNOLOGY

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

- The composite organization employs five risk analysts who identify threats, quantify risks, define risk appetite, and implement preventive measures.
- The risk analysts reduce their investigation time by 75% with DTEX.
- The average fully burdened annual salary for an insider risk analyst is $168,000, which includes a 1.35x multiplier to account for overhead costs.
- The risk analysts recapture 50% of the productive hours gained and dedicate that to other value-add activities.

Risks. Forrester recognizes that these results may not be representative of all experiences. The impact of this benefit will vary depending on:

- Insider risk program complexity, maturity, and expertise.
- Insider risk analyst expertise and compensation.
- Prior solutions.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $705,000.

75%

Reduction in investigation time with DTEX

"DTEX reduced the number of false positives, which reduces the time spent [on investigations]. We have fewer investigations than we did before because we have better context."

VP OF CYBERSECURITY, BANKING

"DTEX is more predictive, provides better quality escalations, is more deliberate in assessing risk, and gives us timely response capabilities."

DIRECTOR OF INSIDER RISK, PHARMACEUTICALS

Insider Threat Risk Efficiencies					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Insider risk analysts	Composite	5	5	5
B2	Percentage reduction in investigation time with DTEX	Interviews	75%	75%	75%
B3	Fully burdened annual salary for an insider risk analyst	Composite	$168,000	$168,000	$168,000
B4	Productivity recapture	TEI standard	50%	50%	50%
Bt	Insider threat risk efficiencies	A1*A2*A3*A4	$315,000	$315,000	$315,000
	Risk adjustment	↓10%			
Btr	Insider threat risk efficiencies (risk-adjusted)		$283,500	$283,500	$283,500
	Three-year total: $850,500			**Three-year present value: $705,023**	

UNQUANTIFIED BENEFITS

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

- **Avoided data breach costs.** Interviewees told Forrester that DTEX significantly reduced the risk of data breaches by providing comprehensive, real-time monitoring and analysis of user activities across their organization. DTEX detected anomalies and potential threats early, allowing for proactive intervention before they escalated into data breaches. By continuously assessing user behavior within a wider context, DTEX helped identify insider threats, compromised accounts, and data exfiltration attempts with higher precision than what was possible in interviewees' prior environment. This proactive approach ensured that security teams were alerted to suspicious activities promptly, enabling them to take quick and effective action to mitigate risks.

  Additionally, DTEX's visibility across endpoints and its integration with existing security frameworks enhanced the overall security posture, providing defense mechanisms against potential data breaches and ensuring sensitive data remained protected. The VP of cybersecurity in a banking organization said: "There have been some really big things

that DTEX has identified both from an investigation and alerting standpoint and then from our larger insider threat program standpoint. It has given us detective capabilities in so many situations where there was nothing else. DTEX can whip something up really quickly to show what the detective control looks like."

- **Protected IP.** Interviewees noted that DTEX increased their IP protection by constantly monitoring and analyzing user behavior, detecting potential insider threats, preventing data loss through policy enforcement, facilitating efficient incident response, and ensuring compliance with security protocols and regulations. The director of insider risk at a pharmaceutical organization commented: "DTEX is helping us to protect our crown jewel data that drives our business success. It also enables us to look for accidental and intentional changes that could occur with our IP, drugs, or strategic data that contribute to our success. … It gives us better protection of IP that helps protect our brand for our customers."
- **Improved policy configuration and management.** Interviewees cited that DTEX's out-of-the-box and customizable policies streamlined policy configuration and management. The senior manager of threat intelligence at an energy organization said: "We have reviewed and revamped our organization's policies. We have a secure file transfer protocol (SFTP) tool that we use for business needs, but through the course of the last three months, we have seen people uploading personal data to it. We couldn't have seen it without DTEX."
- **Improved collaboration between security and other teams.** Insider risk spans cross-functional groups, where legal teams are often tasked with providing compliance guidance and HR assists in recognizing insider risks. Interviewees said that DTEX helped strengthened cross-functional collaboration and threat management efforts across cybersecurity, legal, HR, IT, and other related teams. The director of insider risk at a pharmaceutical organization said, "Teams are able to use DTEX data to validate other events, training, lateral movement, HR requests, and leaving worker activities."
- **Reduced shadow IT.** Interviewees noted that they were better able to detect shadow IT with DTEX by collecting and analyzing information on devices, applications, and users. Security teams could then safeguard non-IT systems from internal and external malicious attacks, enhancing the overall security posture. The VP of cybersecurity in a banking organization stated: "We leverage DTEX to elevate privileges on your endpoint.

For example, we built our own custom internal privilege application, and it only allows you to elevate for a certain amount of time. DTEX identifies users who are using that time to download software they shouldn't be. DTEX alerts us to anything that occurs in an identified time frame."

> "We had a [finding] earlier in the year that had visibility all the way up to the SMC [senior management committee]. An individual exfiltrated data using cloud file storage that nobody knew existed, nor did we know there was a bypass in place for it. The sensitivity of that data was enough that our SMC had an interest. We would not have seen that as a company had DTEX not caught it."
>
> **SENIOR MANAGER OF THREAT INTELLIGENCE, ENERGY**

FLEXIBILITY

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

- **Increased AI-readiness.** The senior director of the threat management center at a telecommunications organization said their organization leveraged DTEX to provide insights into risks introduced by ChatGPT, preparing their organization for AI investments and the associated insider risk. The senior director of the threat management center said: "One specific use case that I've started working with DTEX on is with ChatGPT. I have a tool that captures what goes into ChatGPT and what comes out. I can integrate that tool with DTEX, search the content, flag confidential keywords, and be able to give that data to DTEX where we factor in higher risk scores."
- **Enhanced cybersecurity tech stack integrations.** Interviewees extended the value of their investment by taking insights from DTEX and integrating them with other cybersecurity solutions. This integration helped consolidate insights into fewer systems,

which boosted visibility, automation, and productivity. The director of insider risk at a pharmaceutical company said, “We have continuously grown our use cases and further integrated the data into our SIEM solution and SOAR [security orchestration, automation, and response] for incident response.”

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

> “We are exceptionally happy with DTEX and its performance. We are looking forward to seeing further investment in road mapping for enhancements, community collaboration, and customer support.”
>
> **DIRECTOR OF INSIDER RISK, PHARMACEUTICALS**

APPENDIX A: TOTAL ECONOMIC IMPACT

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

Total Economic Impact Approach

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

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

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

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

Present Value (PV)

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

Net Present Value (NPV)

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

Return on investment (ROI)

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

Discount rate

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

Payback period

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

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

APPENDIX B:ENDNOTES

[1] Source: Manage Insider Risk With Zero Trust, Forrester Research, Inc., July 5, 2023.

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

ABOUT FORRESTER CONSULTING

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

FORRESTER®