ESG Economic Validation

Analyzing the Economic Benefits of Proofpoint Insider Threat Management

By Brian Garrett, VP IT Validation Services; and Jack Poller, Senior Analyst, September 2020

Executive Summary

Strengthening cybersecurity continues to be a top business initiative driving technology spending.[1] Yet many organizations are unable to acquire effective cybersecurity tools, and, with the global cybersecurity skills shortage, are equally unable to recruit the requisite staff. This leads to weaknesses or even holes in the organization's cybersecurity defenses, particularly when it comes to insider threats, increasing the risk of compromise.

ESG validated that Proofpoint Insider Threat Management (ITM) effectively addresses the insider threat challenge by generating user-attributed data activity with an easy-to-use timeline view and screen captures. The solution accelerates incident response and remediation, providing substantial cost savings and reducing organizational risk. Proofpoint ITM is also used as the front-end forensic investigation tool for SIEMS and other cybersecurity controls, enhancing user productivity and increasing efficiency.

ESG validated the benefits that Proofpoint ITM customers have experienced through a series of interviews and used the information to create a model scenario that shows that a 10,000-employee organization can reduce the cost of insider threats by almost $400,000 per month through improved productivity, avoidance of risk, and value gained from the platform. ESG's model predicts a 5 month payback period and a 695% three-year return on investment for organizations choosing to implement Proofpoint ITM versus continuing to operate without an insider threat management program.

[1] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.

Introduction

This ESG Economic Validation focused on the quantitative and qualitative benefits organizations can expect by empowering their security operations teams with Proofpoint's suite of intelligence-driven security products to faster and more efficiently analyze, detect, investigate, and respond to insider threats and cyber incidents.

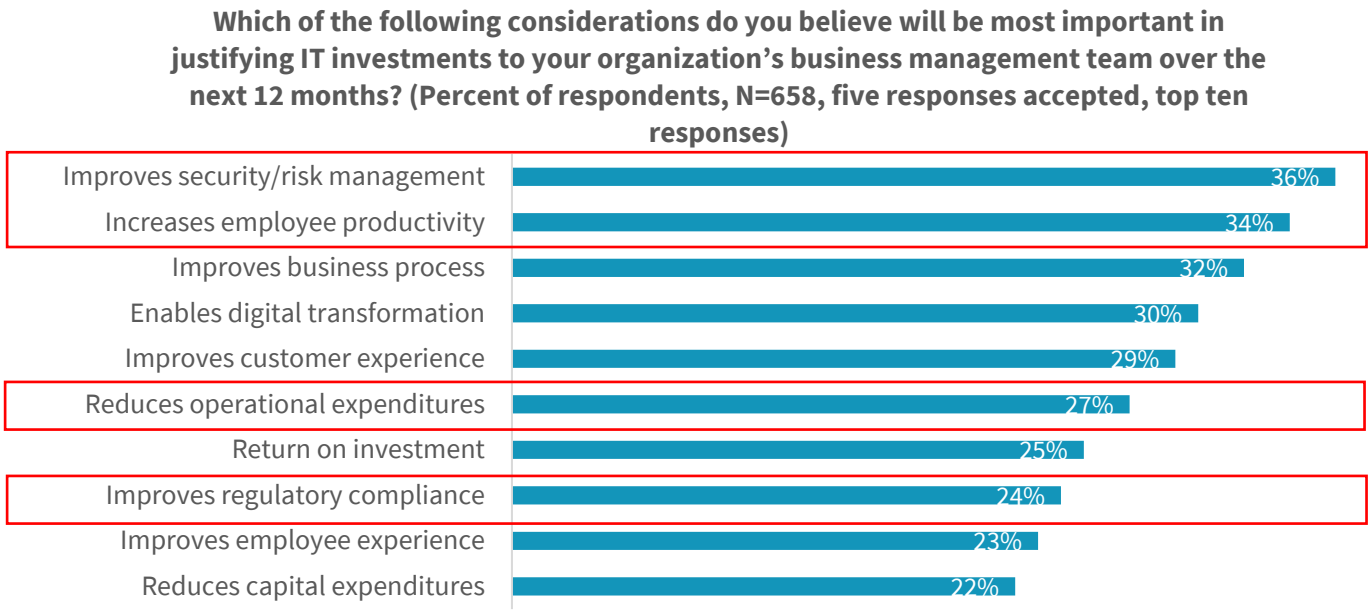
Challenges

While organizations devote a majority of their cybersecurity efforts and budgets to recognize and prevent external threats, they must also be concerned about internal threats and breaches caused by careless or negligent employees or contractors, criminals or malicious insiders, or credential thieves. According to Ponemon research, the number of incidents increased by 47% and the cost of insider threats increased 31% over the last two years, with organizations suffering an average annualized loss of $11.45 million.[2]

Protecting an organization from insider threats has become more difficult due to the rapidly changing and evolving threat landscape, the growing attack surface as organizations shift to support mobile and remote workers, and the increased complexity of IT infrastructures. These challenges are exacerbated by the global cybersecurity skills shortages, with 44% of organizations surveyed by ESG reporting a problematic shortage of cybersecurity skills,[3] making it harder for organizations to appropriately staff cybersecurity teams.

Thus, CISOs, CIOs, and IT managers are looking for solutions that can simultaneously increase security and efficiency. According to ESG research, 36% of organizations indicated that improving security and risk management was one of the considerations that will be most important in justifying IT investments to their business management teams over the next 12 months, making it the most cited response (see Figure 1). Additional considerations for justifying IT investment include increasing employee productivity (34%), reducing OpEx (27%), and improving regulatory compliance (24%).[4]

Figure 1. Top Ten Most Important Considerations for Justifying IT Investments



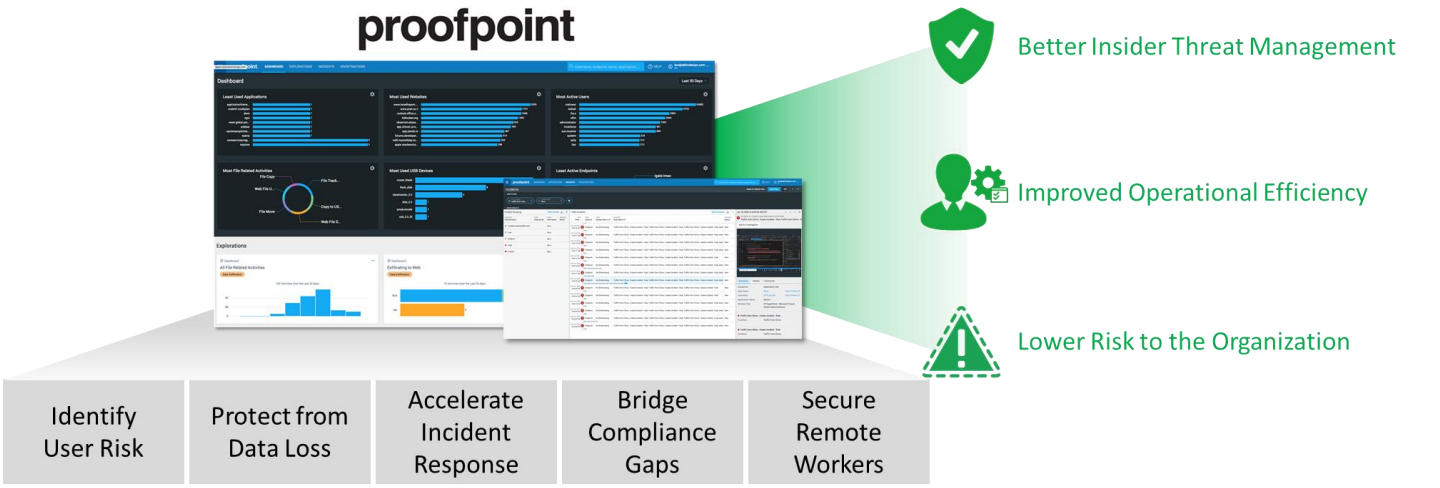
Source: Enterprise Strategy Group

[2] Source: The Ponemon Institute, *2020 Cost of Insider Threats: Global Report.*
[3] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.
[4] Ibid.

The Proofpoint Solution

Proofpoint Insider Threat Management (ITM) uses a people-centric approach to user risk analysis, aggregating and organizing data for each individual user to increase efficiency and fidelity of threat analysis. Proofpoint ITM user risk analysis consists of three key elements: user risk profiling, cross-channel visibility, and activity timelines.

Figure 2. The Proofpoint Insider Threat Management Platform



Source: Enterprise Strategy Group

Proofpoint ITM provides:

- Context—to correlate user activity, data interaction, and user risk, with timeline-based visualizations and screen recordings of potentially malicious activity for people-centric user risk analysis.
- Detection—of insider threats via data exfiltration, privilege abuse, application misuse, unauthorized access, accidental activity, and other anomalous activity.
- Investigation—to accelerate incident response with workflows and evidence presented in easy-to-understand visualizations around user-driven events, fostering collaboration between security, IT, legal, regulatory, and other teams.
- Modern architecture—with APIs, enhancing scalability, security, and privacy, and providing flexible SaaS or on-premises deployment.

The use cases for Proofpoint ITM include:

- Identify User Risk—User risk profiling with data organized around the user enables the organization to focus attention on higher-risk users based on alert history, privilege levels, HR watch lists, non-employees, and whether a user is a frequent recipient of attacks. Aggregating user activity, user data accesses, live threat research, and activity timelines enables automatic correlation with the context to identify and understand user risk.
- Protect from Data Loss—Policy-based rules can trigger alerts and automated actions. Proofpoint includes more than 400 scenario-based alerts drawn from security researchers and crowdsourced threat intelligence, enabling organizations to stop data loss, such as the copying of sensitive data to USB drives or attaching of files to cloud-based email services. Security teams can define their own scenarios, alerts, and actions to tune data loss prevention to their unique environment.

- Accelerate Incident Response—Proofpoint's user-centric approach provides the necessary context to identify the who, what, when, where, and why of cyber incidents. This enables organizations to disambiguate between machine- and user-instigated activity as well as understand the full context to assess whether an alert represents a credible risk, accelerating the time to respond to incidents.

- Bridge Compliance Gaps—Proofpoint ITM provides the necessary visibility into user activity and data interaction to identify and prevent data exposure including personally identifiable information (PII), payment card industry (PCI), and protected health information (PHI), enhancing an organization's compliance with data and privacy standards, mandates, and regulations. Proofpoint includes role-based access controls (RBACs), anonymization of collected data, and the ability to exclude certain activities from monitoring, further enhancing compliance.

ESG Economic Validation

ESG completed a quantitative economic validation and modeled analysis on the Proofpoint ITM platform.

ESG's Economic Validation process is a proven method for understanding, validating, quantifying, and modeling the economic value propositions of a product or solution. The process leverages ESG's core competencies in market and industry analysis, forward-looking research, and technical and economic validation. ESG reviewed the results of existing case studies and end-user surveys and conducted in-depth interviews with end-users to better understand and quantify how Proofpoint ITM has impacted their organizations, particularly in comparison with how they used to operate prior to deploying Proofpoint ITM or previous experiences at other organizations. The qualitative and quantitative findings were used as the basis for a simple ROI model comparing the expected savings and benefits that a modeled organization might expect versus the expected cost of deploying Proofpoint ITM.

Proofpoint ITM Economic Overview

ESG's economic analysis revealed that customers who had deployed Proofpoint ITM were very satisfied with the product and felt that they had greatly streamlined their security operations, were operating more efficiently, and were doing a better overall job at protecting the organization. ESG found that Proofpoint ITM provided its customers with significant savings and benefits in the following categories:

- Lower Operational Cost of Insider Threat Management—Proofpoint ITM's user-centric focus, timeline views, and screen recording accelerated detection of insider threat incidents, simplified forensic investigations, guided remediation, and helped explain incidents to non-technical professionals.

- Improved Security Effectiveness and Reduced Risk to the Organization—With faster identification and response to insider threats and cyber incidents, Proofpoint ITM can reduce the number of incidents, reducing risk and strengthening cybersecurity.

- Lower Operational Cost of SecOps—Customers found that using Proofpoint ITM as the forensic investigation front-end to SIEM and other cybersecurity alerts and incidents simplified and accelerated incident response. Proofpoint was also deployed to provide audit trails and improve compliance.

Lower Operational Cost of Insider Threat Management

Customers whom ESG spoke with reported that Proofpoint ITM significantly reduced the time to detect and investigate insider threat incidents and was able to disambiguate between machine and human activity, further accelerating investigatory efforts and reducing associated costs.

- **Easier investigation and documentation of end-user activity**—Customers reported that Proofpoint ITM simplified and accelerated the forensic investigation of alerts. Rather than spending days reviewing and cross correlating logs from endpoints, servers, network monitors, and security controls to validate an alarm, analysts were using Proofpoint ITM's timeline and screen captures to identify and remediate malicious or inadvertent yet damaging user activity in real time. The timeline view and screen captures proved to be self-explanatory for non-technical professionals accelerating HR and legal investigations. When presented with Proofpoint ITM evidence, malicious insiders often dropped their challenge to HR or legal actions.

"Traditional security tools tell you what the machine did, not what the human did."

CISO, Global Private Equity

- **Faster detection of potential insider threats**—One CISO of a global private equity firm said, "Theft in my business is somewhat contextual. They're not running command shells or hacking. They're taking a document and sending it to a relative at a competitor. No amount of DLP or behavior analysis will show that. And so that's where we came with the mantra that 'you can't log everything.' Other tools that do behavior analysis require you to log everything." Proofpoint ITM's analysis engine proved to be adept at detecting insider threat activity, especially activity that may be valid or malicious depending on context. While printing, attaching files to email, or transferring files to network attached storage is routine legitimate activity, such actions may also be malicious depending on context, and will not be captured by traditional security controls when the user works from home. The ability to collect and analyze user activity in addition to machine activity accelerates identification of potentially harmful incidents.

- **Faster cyber incident response**—All the CISOs we spoke with said that Proofpoint ITM's screen capture and timeline features enabled them to quickly identify affected compromised accounts and exfiltrated data. Thus, they were able to rapidly remediate incidents, limiting exposure and recapturing lost data.

"Before we deployed Proofpoint ITM, it took a couple of weeks to get user-attributed data activity; now it takes about 30 minutes."

CISO, Global Defense Contractor

Improved Security Effectiveness and Reduced Risk to the Organization

Customers whom ESG spoke with reported that, by accelerating time to respond and shrinking the impact of compromise, Proofpoint ITM improved security effectiveness and reduced risk to the organization.

- **Faster response to insider threats and cyber incidents**—Proofpoint's alerts work in concert with the timeline view and screen captures to simplify alert investigations, accelerating the organization's response to threats and incidents.

- **Reduced risk of compromise**–Employees and contractors are less inclined to commit malicious acts when they know their activity is monitored and logged and they have a higher probability of being caught.

- **Reduced impact of compromise**—According to one customer, traditional UEBA tools were terrible at identifying malicious activity because human behavior with malicious intent is so varied that one example of malicious intent doesn't look like the next one. Proofpoint ITM enables customers to rapidly identify and remediate malicious human activity and protect the associated intellectual property, reducing the impact of malfeasance.

- **Reduced risk and impact of insider threats**—Customers indicated that Proofpoint ITM helps the organization to focus attention on higher risk users based on a variety of factors such as access to key intellectual property and sensitive data. Proofpoint ITM also helps prioritize events and incident response activities and reduces dwell time by accelerating incident response and remediation activities.

"Tracking user attributed data activity with Proofpoint ITM is reducing our expected losses due to insider threats and cyber-attacks. It's also helping inform what we need to do for cyber risk insurance."

CISO, Global Risk Management

Lower Operational Cost of SecOps

Every organization that we spoke with felt that Proofpoint ITM had helped them transform their organization to make the most of the resources they had. They reported that their teams were far more productive and were better able to communicate with the business and their peers.

- **End-user activity context for faster time to respond to cyber incidents**—All customers ESG spoke with said they extended their use of Proofpoint ITM for forensic investigations of alerts generated by SIEM and other cybersecurity tools. Instead of requiring a high-level analyst to manually develop a timeline from event logs, Proofpoint's timeline view and screen captures enabled even junior analysts to understand a cyber incident and quickly determine if an alert was the result of human activity, and whether the human action was inadvertent or malicious.

- **Less tier three and four analyst involvement for insider threat and cyber incident investigation**—Proofpoint ITM lowers the barriers of entry for understanding user-attributed data activity for data analysts, enabling initial investigations of alerts to be conducted by tier one and tier two analysts, freeing tier three and tier four analysts to address root causes and handle highly sensitive employee investigations. According to one CISO, 10-15% of work for tier three and four analysts has been transferred to tier one and two analysts, and they're sure that will increase with time and experience.

"My tier 1 and 2 investigators are able to investigate and prioritize events in a more effective manner."

CISO, Global Risk Management

- **Understanding user behavior rather than what the machine was doing**—Traditional security tools work from logs of machine activity and cannot attribute activity to a human. And traditional security tools may not have access to proprietary or encrypted environments. Proofpoint ITM captures actual human activity at the endpoint, regardless of the environment, and the ability to differentiate between human and machine activity is critical to identifying, preventing, and remediating insider threats.

- **Better collaboration with peers**—According to one CISO, Proofpoint ITM lowered the barriers of entry for understanding user-attributed data activity for the security analysts, fostering collaboration among the team. It also made that data more available, more digestible, and more actionable for the non-technical parts of the organization.

- **Increased auditability and compliance**—Tracking changes to web applications can be difficult. Many SaaS applications fail to capture a sufficient audit trail of back-end changes. Other systems provide a single admin account with sysadmins using a shared password. We found that customers use Proofpoint ITM to identify administrative access to applications and trigger additional actions to log activity and use screen capture to augment the audit trail. Using Proofpoint ITM enhances compliance and auditability and enables organizations to attribute actions to actual users rather than to a shared administrative account.

"Highly sensitive employee investigations would take 8-10 hours to comb through SIEM and endpoint logs; now it's down to 30 minutes or less."

CISO, Global Private Equity

ESG Analysis

ESG leveraged the information collected through vendor-provided material, public and industry knowledge of economics and technologies, and the results of customer interviews to create a three-year ROI model that compares the costs and benefits of implementing Proofpoint ITM with continuing to operate without an insider threat management platform. ESG's interviews with Proofpoint ITM's customers, combined with experience and expertise in economic modeling and technical validation of Proofpoint ITM products helped to form the basis for the modeled scenario.

ESG's modeled organization consisted of a cybersecurity team with varying degrees of experience providing security services to an organization with 10,000 employees. ESG factored in the expected annual subscription costs for 10,000 endpoints and the cost to install, implement, and train employees to use the Proofpoint ITM platform over a three-year period.

"Proofpoint ITM has definitely had a positive impact for our organization. It lowered the barriers of entry for understanding user-attributed data activity for our security analysts. It also made it more available, more digestible, and more actionable for the non-technical parts of the organization."

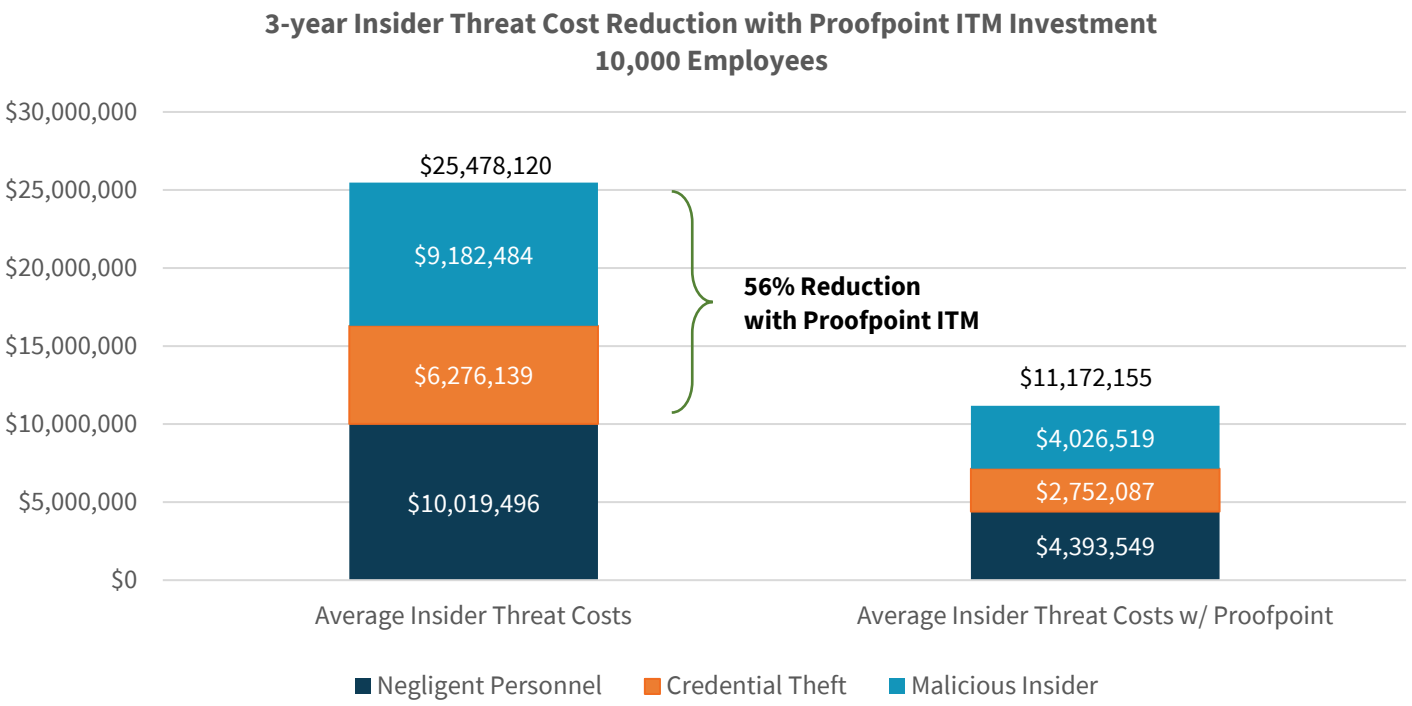
CISO, Global Defense Contractor

On the benefits side, ESG used Ponemon research to model the cost of insider threats. We modeled three insider threat incidents: employee or contractor negligence, criminal and malicious insider attacks, and credential thefts. We then modelled the avoided cost of insider threats achieved through the lower operational costs of insider threat management and security operations achieved by deploying Proofpoint ITM.

According to Ponemon research, the cost of an insider threat can be distributed across various activities, including containment, remediation, incident response (IR), investigation, monitoring and surveillance, escalation, and ex-post analysis. Similarly, the cost of an insider threat can be distributed across standardized categories, including direct and indirect labor, technology, disruption and downtime, process or workflow changes, cash outlays, revenue losses, and overhead.[5] Using Ponemon research about the distribution of costs for these activities and the average costs incurred for each of the incident types, ESG's model predicted a 56% reduction in insider threat costs over three years based on the decrease in time and effort for these activities, as shown in Figure 3. This reduction averages almost $400,000 per month for a 10,000-employee organization.

[5] Source: The Ponemon Institute, *2020 Cost of Insider Threats: Global Report.*

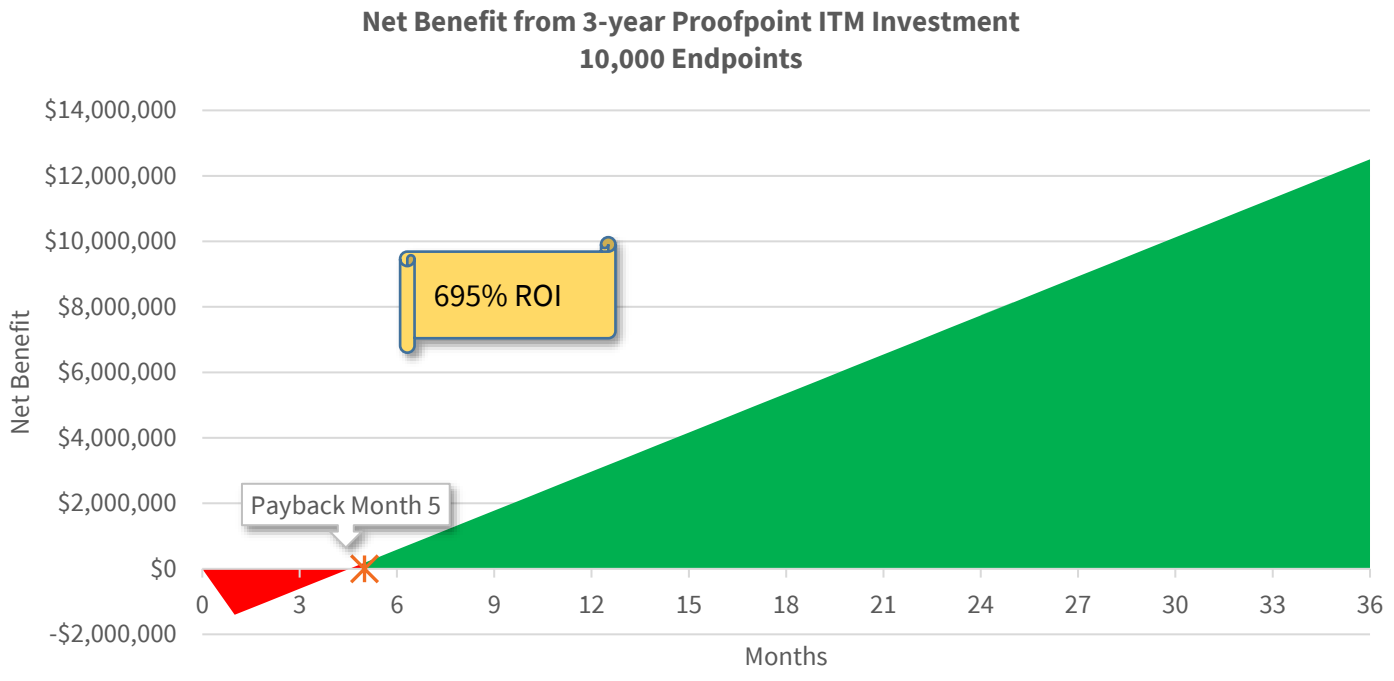
Figure 3. Three-year Insider Threat Cost Reduction with Proofpoint ITM



Source: Enterprise Strategy Group

ESG modeled the net benefits to the organization based on a three-year deployment. As shown in Figure 4, the savings in insider threat costs will pay back the initial investment in less than six months, and the resulting benefit to the organization is a three-year ROI of 695%.

Figure 4. Net Benefit from 3-year Proofpoint ITM Investment



Source: Enterprise Strategy Group

What the Numbers Mean

ESG's analysis predicted substantial savings and benefits for our modeled organization. While no modeled scenario could ever accurately represent the economics behind every deployment, ESG encourages organizations to perform their own analysis to see how much they can save. ESG suggests that organizations consider the following insider threat costs factors identified by Ponemon research that were included in our analysis (see Table 1).[6]

Table 1. Insider Threat Cost Factors and Savings

Costs by Activity Center	% of Insider Threat Costs	Costs by Standardized Categories	% of Insider Threat Costs
Containment	33%	Direct and indirect labor	25%
Remediation	23%	Technology (amortized)	21%
Incident response (IR)	18%	Disruption and downtime	18%
Investigation	16%	Process or workflow changes	15%
Monitoring and surveillance	4%	Cash outlays	10%
Escalation	3%	Revenue losses	6%
Ex-post analysis	3%	Overhead	4%

Source: The Ponemon Institute

Issues to Consider

ESG's economic analysis looked at hard costs incurred by an organization from insider threats and the savings in costs when deploying Proofpoint ITM. ESG also suggests that organizations investigate areas ESG did not include in the ROI model, including:

- **Risk reduction**—The probability of risk from insider threats may be reduced when deploying Proofpoint ITM, especially when potentially malicious employees or contractors are aware that user activity may be monitored.
- **Forensic investigation—**Proofpoint ITM customers reported that the platform reduced the time and effort of forensic investigations of alerts generated by SIEM and other security controls.
- **Legal—**Proofpoint ITM customers reported that the platform simplified the effort of explaining an incident to non-technical personnel and that, when faced with evidence provided by Proofpoint ITM, malicious insiders may stop their challenges to HR and legal actions.
- **Compliance—**Proofpoint ITM may complement traditional DLP solutions, helping to prevent data loss without the cumbersome and time-consuming effort of identifying and classifying all sensitive data. Further, Proofpoint ITM can be used to generate audit trails and activity attribution for SaaS, web, and other apps that do not automatically capture administrative activity or use a shared administrative account.

The Bigger Truth

Strengthening cybersecurity has consistently topped ESG research respondents' list of business drivers for technology spending for several years.[7] As organizations continue to grow and organize their teams, and invest in new solutions, one thing is clear: The problem is not a lack of security tools and threat intelligence, but a lack of human power to effectively manage, interpret, and take action based on the intelligence and alerts. Modern security organizations require an insider

[6] Source: The Ponemon Institute, *2020 Cost of Insider Threats: Global Report.*

[7] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.

threat management platform that can help streamline the security process, automate repetitive tasks, provide AI-driven intelligence, and allow the human resources to become more operationally efficient.

ESG validated that Proofpoint Insider Threat Management provides customers with a platform that helps them get the most out of their security investments. Security teams are far more empowered, productive, and focused on the most important tasks; their investments in their SIEM and other security products are easily integrated and enhanced to provide even greater value; and their threat intelligence feeds are ready to evaluate, purchase, and integrate. Customers reported considerably improved visibility and a greater ability to share threat intelligence internally with other divisions of the company, and externally with their peers and security organizations.

ESG's modeled cost-benefit analysis shows that an organization that implements Proofpoint ITM can expect to save through improved security team productivity, value added from included threat intelligence products, and avoidance of risk. The key assumptions in the model were based on ESG's validation with Proofpoint ITM's customers. ESG's model for a 10,000-employee organization calculated an expected 56% reduction of insider threat costs, averaging almost $400,000 per month, with a five month payback period and an expected return on investment (ROI) of 695%.

Proofpoint ITM does not compete with an organization's existing security products or look to functionally change the way teams need to operate. Instead, Proofpoint ITM serves to operationalize and enhance SIEMs, threat intelligence, cybersecurity controls, and other tools and solutions to make security teams more efficient and to expand the security discussion to other parts of the business. Every organization that ESG spoke with felt they accomplished far more with a smaller team and scaled operations far beyond what was realistically achievable through manpower alone. Some had even brought Proofpoint ITM with them into new roles: The CISO of a global risk management firm said, "I had used Proofpoint ITM in a previous role, and when I came here, I said If we don't have Proofpoint ITM, we are not going to be able to accomplish our goals." As an analyst, you quickly learn that a statement like that is the mark of a transformative technology. If you are looking to transform and streamline your security operations and get the most from your cybersecurity stack, ESG recommends that you contact Proofpoint to see if it is the right insider threat management platform for your team.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.