

ECONOMIC VALIDATION

# Analyzing the Economic Benefits of Trend Vision One

Minimize Cyber Risk, Accelerate Detection and Response, and Improve Overall Operational Efficiency With a Proven Cybersecurity Platform

By Nathan McAfee, Senior Economic Analyst  
Enterprise Strategy Group

January 2024

# Contents

**Introduction**..... 3

    Challenges..... 3

    The Solution: Trend Vision One ..... 4

**Enterprise Strategy Group Economic Validation** ..... 5

    Trend Vision One Economic Overview ..... 5


        Reduced Risk ..... 5

        Improved Detection and Response..... 7

        Improved Operational Efficiency ..... 8


    Enterprise Strategy Group Analysis ..... 10

**Conclusion**..... 10




## Economic Validation: Key Findings Summary


Validated Benefits of Trend Vision One



**Reduced risk of data breach of 17%**



**Reduction in security FTE costs of 70%**



**Reduced customer churn by 5% and security employee turnover by 20%**

- **Reduced Risk:** Trend Vision One provides insight and clarity into IT assets, integrations, and user behaviors that lowers overall risk.
- **Improved Detection and Response:** Trend Vision One customers report the elimination of alert fatigue, enabling them to focus on actual threats and remediate issues faster than in the past.
- **Improved Operational Efficiency:** ESG found that customers deploying Trend Vision One can shift FTE focus to above-the-line activities that better align IT capabilities with business goals.

# Introduction

This Economic Validation from TechTarget’s Enterprise Strategy Group (ESG) is focused on the quantitative and qualitative benefits organizations can expect by using Trend Vision One when compared to fragmented cybersecurity strategies to improve security posture and protect, detect, and respond to security threats and events.

## Challenges

Securing digital assets and IT resources is a challenge that is increasing in complexity at a rate that can seem exponential. With each change in the digital landscape, attack vectors are created that must be located, understood, and secured. ESG studied challenges companies face concerning cybersecurity and found these to be consistent across most companies and their cybersecurity teams:

- **Alert fatigue.** Cybersecurity teams are often faced with alert numbers that can exceed 1 billion logs generated per 1000 devices each week, the sheer magnitude of identifying true risks can overwhelm most systems and security teams.
- **Shift in the location of IT resources.** ESG research found that 60% of organizations have different teams responsible for on-premises, public, and private cloud resources.<sup>1</sup> This creates differing strategies across an IT ecosystem, often leading to short-sighted decisions that create technical debt. Additionally, as hybrid workforces become the norm, the number of locations that must be supported has grown to the point that each employee is their own location and often outside the protective realm of corporate networks or company-provided hardware.
- **Increasing complexity.** As IT environments become more complex, systems used to detect, respond to, remediate, and contain threats can become stretched and ineffective. The result is an increase in the time to find and remedy threats—and, even worse, a lack of visibility of active risks. ESG research found that almost a quarter of companies (23%) employ more than 25 different cybersecurity products.<sup>2</sup> This leads to digital silos, increased complexity, and gaps in coverage, and it is often accompanied by short-sighted decision-making that creates technical debt.
- **Massive growth in SaaS applications.** Few applications are self-contained. As inter-functionality is incorporated into applications using APIs, third-party software, and multiple development teams, the threat landscape of those applications increases. ESG research shows that 76% of applications developed have more than 25 APIs associated with them, with up to 75% being changed at least weekly.<sup>3</sup> This increases the number of attack vectors and forces companies to assume the security risk of the external resources connected through the API.<sup>4</sup>
- **Risk of unknown resources.** It is a challenge to identify all digital assets, especially with the ongoing demands in protecting remote workforces. Without a clear view of what assets make up the organizational attack surface, securing them is impossible.
- **Increasing complexity of bad actors.** Attacks are increasing in sophistication and volume. ESG found that 68% of organizations have fallen victim to an attack that used encrypted traffic in an attempt to avoid

<sup>1</sup> Source: Enterprise Strategy Group Research Report, [Network Security Trends in Hybrid Cloud Environments](#), July 2022.

<sup>2</sup> Source: Enterprise Strategy Group Complete Survey Results, [ESG/ISSA Cybersecurity Process and Technology Survey](#), June 2022.

<sup>3</sup> Source: Enterprise Strategy Group Research Report, [Securing the API Attack Surface](#), August 2023.

<sup>4</sup> Ibid.

detection.<sup>5</sup> Encryption is a cornerstone of security methodology but is no longer the fail-safe preventative measure it was in the past.

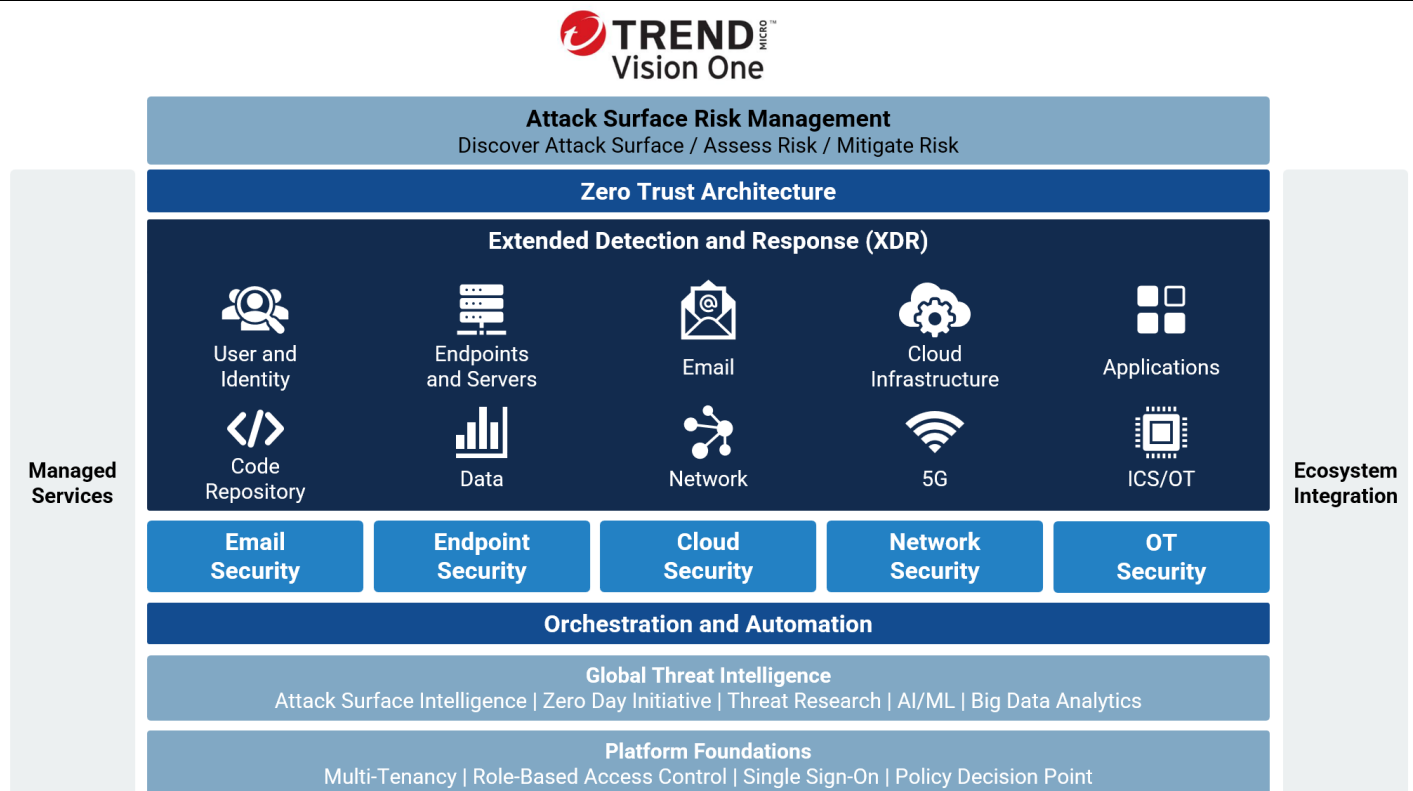
- **Escalating impact of security events.** The impact of security events ranges from simple distractions to ransomware events that average \$4.45M per occurrence.<sup>6</sup> Data shows that companies that experience successful attacks underperform the market by an average of 11.9% in the two years following an attack.<sup>7</sup>

The challenges are clear. Threats are increasing in quantity and sophistication, and attack surfaces are expanding as new devices, cloud assets, SaaS applications, IP and domain locations, data types, and more are being added. Companies need a solution that simplifies proactive, risk-based protection and threat detection across all use cases.

## The Solution: Trend Vision One

As shown in Figure 1, Trend Vision One is a modern, purpose-built, AI-powered cybersecurity platform that leverages the combined power of full lifecycle attack surface risk management solutions, XDR, leading global threat intelligence, AI/ML technology, and zero trust principles to bridge comprehensive threat prediction, prevention, detection, and response capabilities for superior protection against cyberthreats.

Figure 1. Trend Vision One Combines Prevention, Detection, Response, and Protection



Source: Trend Vision One

<sup>5</sup> Source: Enterprise Strategy Group Research Report, *The Evolving Role of Network Detection and Response*, March 2023.

<sup>6</sup> Source: IBM Corporation, *Cost of a Data Breach Report 2023*, July 2023.

<sup>7</sup> Source: Keman Huang et al., *Harvard Business Review*, "The Devastating Business Impacts of a Cyber Breach," May 4, 2023.

Organizations that adopt Trend Vision One find this comprehensive cybersecurity platform can achieve a shift toward proactive security to better detect, manage, and mitigate security threats across their environment.

## Enterprise Strategy Group Economic Validation

Enterprise Strategy Group (ESG) completed a quantitative economic analysis on the impact that Trend Vision One can have on an organization's ability to meet IT and business goals.

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 conducted in-depth interviews with end users to better understand and quantify how Trend Vision One has affected their organizations, particularly in comparison with previously deployed and/or experienced solutions. The qualitative and quantitative findings were used as the basis for a simple economic model comparing the expected costs of security and event infrastructure of Trend Vision One with traditional on-premises and cloud-based services.

### Trend Vision One Economic Overview

ESG economic analysis revealed that Trend Vision One provides its customers with significant savings and benefits in categories including the following:

- **Reduced risk.** ESG found that Trend Vision One customers had a lower likelihood of ransomware and breach events as well as reduced impact of actual events.
- **Improved detection and response.** Customers reported a significant improvement in the ability to detect issues that create the highest level of risk and remediate those issues in less time with Trend Vision One.
- **Improved operational efficiency.** Trend Vision One customers found that their overall security and incident response spend was lower when compared with their previous solutions.

### Reduced Risk

The key measurement of any security platform is its ability to secure an IT ecosystem. ESG's analysts studied the before-and-after environments for organizations that have adopted Trend Vision One. In addition to metrics that could be compared side by side, ESG found an entire group of new measurables for Trend Vision One customers to consider. With Trend Vision One, customers were able to proactively secure entire classes of digital assets—including devices, servers, domain and IP addresses, cloud assets, and APIs—that were left under-protected, or even unprotected, in the past. In addition, customers interviewed for this analysis shared benefits in reduced risk, including:

**“Vision One wasn't a replacement for old functionality; it allows us to see things that we were completely unaware of with our old solution. We are scanning and fixing threats that we never would have seen in the past until it was too late.”**

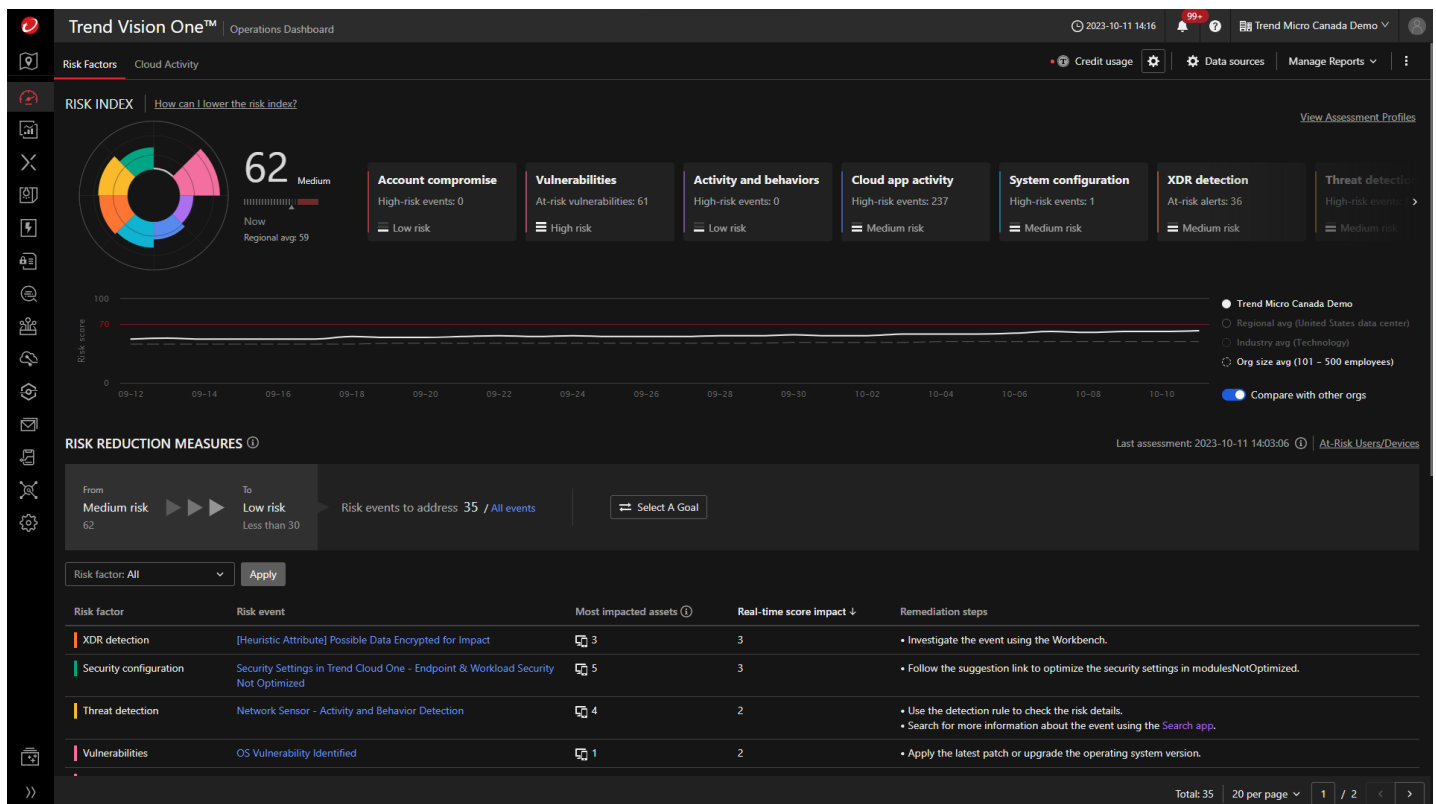
—Security Manager, State Library Systems

- **Lowered chance of breach.** As cited above, one of the top studies in quantifying risk estimates the average cost of a data breach to be \$4.45M. ESG's financial model used 11% as the annual exposure to a breach. Based on customer interviews, that annual risk number was reduced to 8% with Trend Vision One, resulting in an annual benefit of \$1.30M in alleviated risk exposure. When asked why they felt their risk exposure was lowered with Trend Vision One, every participant mentioned improved visibility, improved alert fidelity, and shorter dwell time, which was found to be lower by an average of 65% when compared with their previous environment. One interviewee shared that the focus of the impact of a breach should go far beyond the cost metrics: *“A security issue impacts our reputation. Numbers matter, but the real risk is how our customers view us and our commitment to security.”*

- Improved visibility/insight.** In every conversation ESG had with customers about the impact of Trend Vision One, one of the top benefits mentioned was the improved visibility of their entire security posture and their newfound ability to proactively manage risks. This visibility and risk tracking acts as a centralized source to bring consistency in security posture across all asset types. Customer interviews included a consistent sentiment: *“Before Trend Vision One, we just didn’t know.”* In fact, Trend Vision One provided multiple examples of unmonitored, or even unknown, assets on their network. Another Trend Vision One capability that was specifically called out as a game-changer was the operations dashboard (shown in Figure 2). This feature provides a comprehensive view of the security status and risks in an organization’s devices and accounts, with the ability to dig into each area for specific details. Thus, Trend Vision One’s operations dashboard provides a consolidated list of opportunities to improve the overall security posture of the organization.

“Trend Vision One’s operations dashboard gives us our current risk level as well as detailed ways for us to improve our score and harden our security posture. We couldn’t afford to hire the level of expertise to give us this type of insight, but it’s part of Trend Vision One.”  
—Systems Admin, State Government

Figure 2. Operations Dashboard Provides Risk Index Score and Insight for Improvements



Source: Trend Vision One

- **Faster patching.** With hybrid workforces, many IT assets are outside the control of corporate update systems. Interviewees report that Trend Vision One has brought greater proactivity, clarity, and simplicity to their patch strategy by leveraging threat intelligence informed virtual patching, with one saying, *“We have greatly simplified our patch management. We now have clarity in patch coverage and are rolling them out 102 days faster than we were in the past.”*
- **Alignment with major compliance frameworks.** Organizations that operate in compliance-based industries find that Trend Vision One enables them to better remain within guidelines as well as constantly monitor compliance status. One interviewee shared their belief that their exposure to fines was 60% lower with Trend Vision One. In ESG’s financial model, that 60% reduction is an alleviated risk benefit of \$1.2M annually.
- **Protection of third-party integrations.** Each third-party integration brings risk, as the organization must assume the risks associated with the code of that third party. When exploring the impact of using APIs and third-party integrations, one interviewee said, *“Trend Vision One’s third-party integration is fantastic. We often integrate with security components from other vendors. Trend Vision One will create external dynamic lists so that, when a suspicious object is detected, it feeds automatically into our firewall to block the threat. The visibility we have into third-party integrations is a game-changer and allows us to say ‘yes’ to business requests instead of ‘no.’”* Every company interviewed stated that they were more likely to take advantage of third-party integration capabilities, specifically because of the level of insight and protection that Trend Vision One provides.

**“We are more secure since adopting Trend Vision One. In our proof of concept, we saw a huge number of false positives in the alternatives we were considering. With Trend Vision One, we find the threats detected to be far more accurate, and the information far more specific, than what we saw with the competitors.”**

—Infrastructure Manager, U.S.-based Home Builder

### Improved Detection and Response

With millions of logs generated per day and thousands of possible alerts, trying to identify the threats that matter the most is an overwhelming task. ESG interviewed customers to understand their detection and response metrics before and after Trend Vision One. As shown in Table 1, Trend Vision One has had a substantial impact, reducing noise and allowing organizations to focus on the issues that matter. Additionally, companies found that they were able to get alerts from resources that they were completely blind to in the past.

**Table 1.** Comparing Detection, Triage, Investigation, and Remediation Metrics

	Before Trend Vision One	After Trend Vision One
Number of Alerts per Day	1,000	4
Time to Detect (minutes)	11,520	1
Time to Triage (minutes)	480	less than 1
Time to Investigate (minutes)	360	90
Time to Remediate (minutes)	1,860	6
FTEs needed	5.6	less than 1

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

**“We reduced our research time on issues by over 75%. Now we work faster and respond quicker to threats. However, it isn’t an apples-to-apples comparison to our old environment. With Trend Vision One we are finding and fixing threats that we couldn’t see or understand in the past.”** —Information Security Manager, U.S.-based University System

## Improved Operational Efficiency

Every organization faces the challenge of getting as much impact as possible out of every dollar spent. With Trend Vision One, cybersecurity and IT teams were able to be more proactive in their approach with a platform-based security approach. This impact enabled benefits in the following areas:

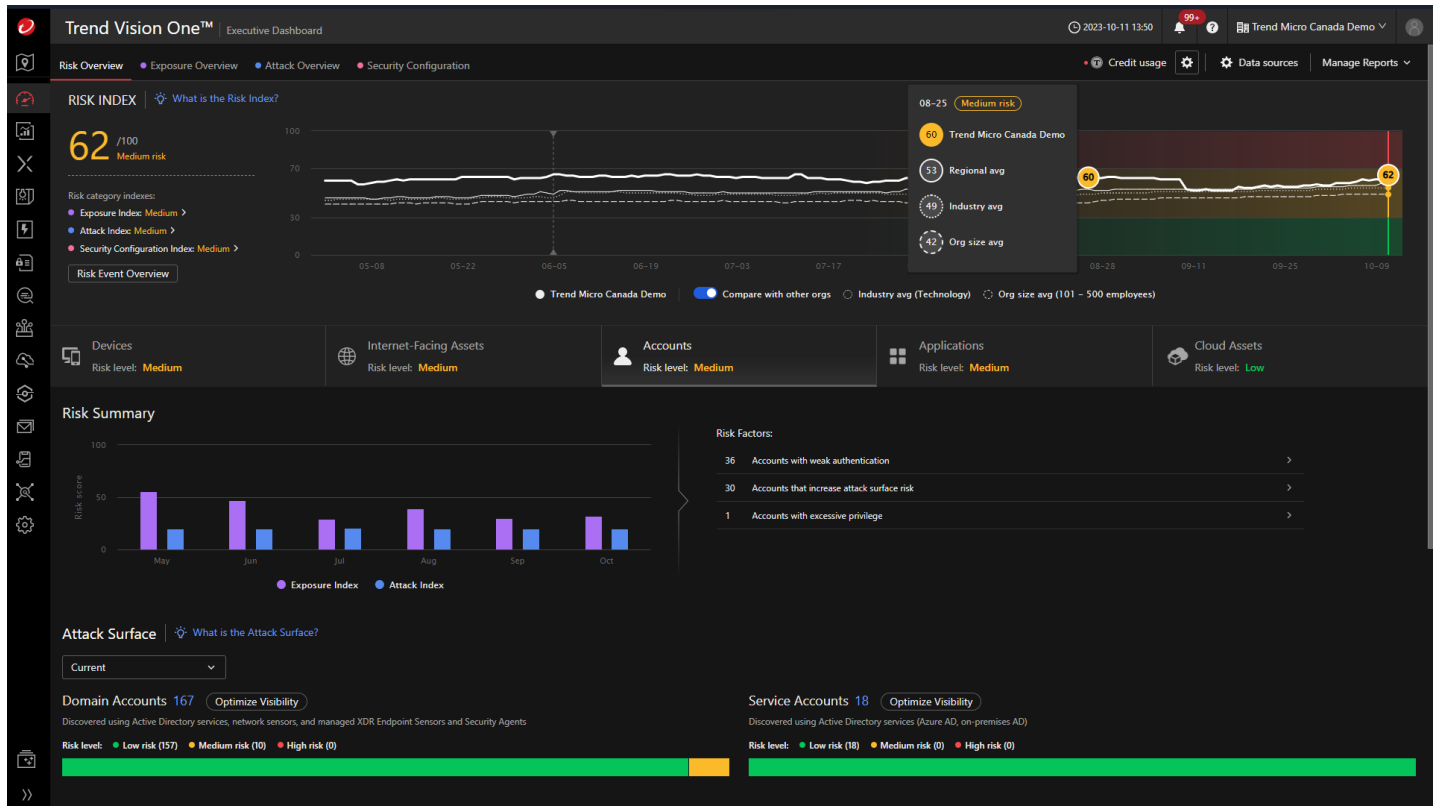
- Improved FTE efficiency.** Each organization interviewed stated that the headcount needed for their cybersecurity platform was lower with Trend Vision One by an average of 70% across all interviewees. One of them shared, *“We used to need eight security analysts to do a far lower level of protection than we can do with two people using Trend Vision One, and these two are far more empowered.”* In ESG’s economic model, this results in \$1.04M annual savings. When shifting the conversation to support costs, with Trend Vision One the model saw the 28 support staff reduced to 17, resulting in \$864K annual savings.
- Management insight.** Trend Vision One has a built-in executive dashboard that allows CIOs, CISOs, and managers to access an overview of companywide cyber-risk trends and threats at a glance, plus the ability to explore each metric as deeply as they would like. One interviewee shared, *“Executive dashboard is a fantastic tool to allow execs instant visibility into our status and allows them to dig into details as much as they like, without the need to randomize one of our staff. This alone saves us hours per week and allows them to make more informed decisions.”* As shown in Figure 3, the clarity and insight the dashboard provides can be modified to fit the level and needs of the manager, and it has made it easier for cybersecurity leaders to communicate up to nontechnical peers and boards of directors.
- Improved customer satisfaction.** Customers pay attention to security breaches and value interactions that are secure while maintaining a fluid user experience. Interviewed customers estimate they have been able to reduce their customer churn from 6% down to 5.7%, specifically because of the protections that Trend Vision One provides as well as the way that Trend Vision One enables third-party integrations. In ESG’s economic model, this 0.3% improvement in customer churn results in an annual benefit of \$2.43M.

**“Our security teams were constantly facing a backlog of new things that must get implemented on our network. Just doing risk assessments on these new items took more time than we have. With Trend Vision One, we saw our workload drop by 70%, freeing up time to work with our business units to better align their goals with IT capabilities.”**

—Information Security Manager, U.S.-based University System



Figure 3. Executive Dashboard Provides Updated Status With Ability to Dive for Details



Source: Trend Vision One

- Improved employee satisfaction.** Interviewees report a large shift in employee satisfaction with Trend Vision One. ESG uncovered multiple stories of employees being more empowered, spending less time on mundane tasks, and shifting focus from below-the-line activities like monitoring logs and basic research to above-the-line activities that solve IT and business problems. Among the companies interviewed, they estimated that their IT turnover has decreased by more than 20% since they adopted Trend Vision One. As one interviewee reported, *“Our people love working in this environment. We have the flexibility to expose them to the right level of challenge based on their skill set and have been able to completely remove much of the mundane work that is traditionally associated with security products by using a platform-based approach and AI-supported workflows.”* ESG’s economic model found this benefit to be \$75K annually.
- Lower security costs.** Trend Vision One brings comprehensive cybersecurity capabilities across the customer environment to a single platform. Some of these capabilities are displacements for existing, siloed point solutions, and some platform capabilities include new category innovations that help harden the overall security posture. Multiple organizations alleviated their product spend, with 40% of interviewed organizations stating they eliminated over \$500K per year in cybersecurity costs.
- Lowered burden of audits.** ESG found substantial benefits in reduced costs needed for compliance and audit work, with our financial model showing a \$207K annual cost reduction in this area. One company shared, *“We used to have four headcounts just for audits. With Trend Vision One, we can do it with just a fraction of a head.”*

## Enterprise Strategy Group 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 TCO/ROI model that compares the costs and benefits of Trend Vision One against a sample modeled company that uses multiple products to provide cybersecurity protection. ESG's interviews with customers who have recently made the transition, combined with experience and expertise in economic modeling and technical validation, helped form the basis for our modeled scenario.

ESG's modeled company is in the high-tech industry, with 15,000 employees and 34,950 endpoints, and it produces \$2.7B in annual revenue. They have 8.4 full-time employees (FTEs) managing their cybersecurity and 28 support analysts. They support 84 locations internationally and are growing at a rate of approximately 3% per year.

### Why This Matters

Every customer interviewed shared that Trend Vision One was not only a replacement for existing products but also a new platform of capabilities that replaced existing point solution deployments, while adding countless new abilities that enabled them to proactively harden their security posture far beyond what it was in the past. ESG did not try to create an old (as-is) environment with all of these added capabilities for comparison; we instead used customer-described scenarios to quantify the impact of switching to Trend Vision One.

## Conclusion

Cyberthreats are growing in frequency and sophistication, while attack surfaces are increasing with new locations, data types, data sources, and use cases. As organizations try to find a cybersecurity solution, they too often end up with a web of products that create silos in some cases and leave gaps in others. This can create an attitude of protectionism that forces business units to work within certain constraints instead of using IT to support new business opportunities. Companies in these scenarios incur unnecessary risk and find short-sighted decisions require continual remediation, which creates technical debt that saps part of future IT budgets. Trend Vision One is a cybersecurity platform that provides comprehensive prevention, detection, and response capabilities to protect users, endpoints, email, applications, networks, clouds, infrastructure, and data. Trend Vision One is underpinned by leading global threat intelligence that few can match and uplevels security analysts at every maturity level with AI-driven guidance to more effectively harden security and thwart cyberattacks.

Enterprise Strategy Group (ESG) analyzed the impact that Trend Vision One can have on an organization's ability to create an environment where cybersecurity is proactive and complete. During this process, ESG interviewed current Trend Vision One customers to understand the challenges they were having in their previous cybersecurity environment and the changes in capabilities they have found with Trend Vision One. ESG found substantial benefits in their ability to lower their risk exposure, streamline their detection and response capabilities, better align IT to business needs, and give management a level of insight that enabled them to make informed decisions without having to distract staff to get updates.

If your organization is looking for an enterprise-level cybersecurity platform that empowers senior leadership, managers, and cybersecurity/IT teams to understand and protect your complete environment, ESG strongly recommends that you explore the capabilities of Trend Vision One.

©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.


Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at [cr@esg-global.com](mailto:cr@esg-global.com).

---

#### About Enterprise Strategy Group

TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

 [contact@esg-global.com](mailto:contact@esg-global.com)

 [www.esg-global.com](http://www.esg-global.com)