Enterprise Strategy Group | Getting to the bigger truth.™

ESG Economic Validation

Analyzing the Economic Benefits of Trend Micro Vision One

By Nathan McAfee, Validation Analyst

May 2021

Executive Summary

Threat detection and response has historically been complex, difficult work. Multiple security point solutions produce increasing numbers of alerts to be triaged. Silos of visibility and investigations hinder data correlation, restrict context, and enable low levels of information sharing. Security teams are forced to manually piece together the story of an attack, delaying response and increasing risk.

The alternative? Extended detection and response (XDR), which provides essential capabilities such as cohesive, enterprise-wide visibility; collection of telemetry from multiple security layers; correlated detection; in-depth investigation; and built-in response actions. Collectively, these capabilities minimize the noise and speed detection and response based on accurate, timely information.

ESG validated that organizations highly aligned with XDR:

- Suffered half as many attacks.
- Were 2.2 times more likely to detect a data breach or successful attack in only a few days or less.
- Were 60% less likely to report attack repropagation.

ESG also validated the positive outcomes experienced by users of Trend Micro Vision One with XDR, including security effectiveness, business enablement, and cost savings. Organizations using the XDR capabilities of Trend Micro Vision One can eliminate siloed views and processes, reduce cybersecurity complexity, pursue new opportunities more confidently, and reduce spending on security products.

This ESG Economic Validation was commissioned by Trend Micro and is distributed under license from ESG.

Introduction

This ESG Economic Validation examines the qualitative and quantitative benefits that organizations can expect from conducting threat detection and response using Trend Micro Vision One and XDR. Organizations can anticipate positive outcomes in security effectiveness, business enablement, and cost reduction.

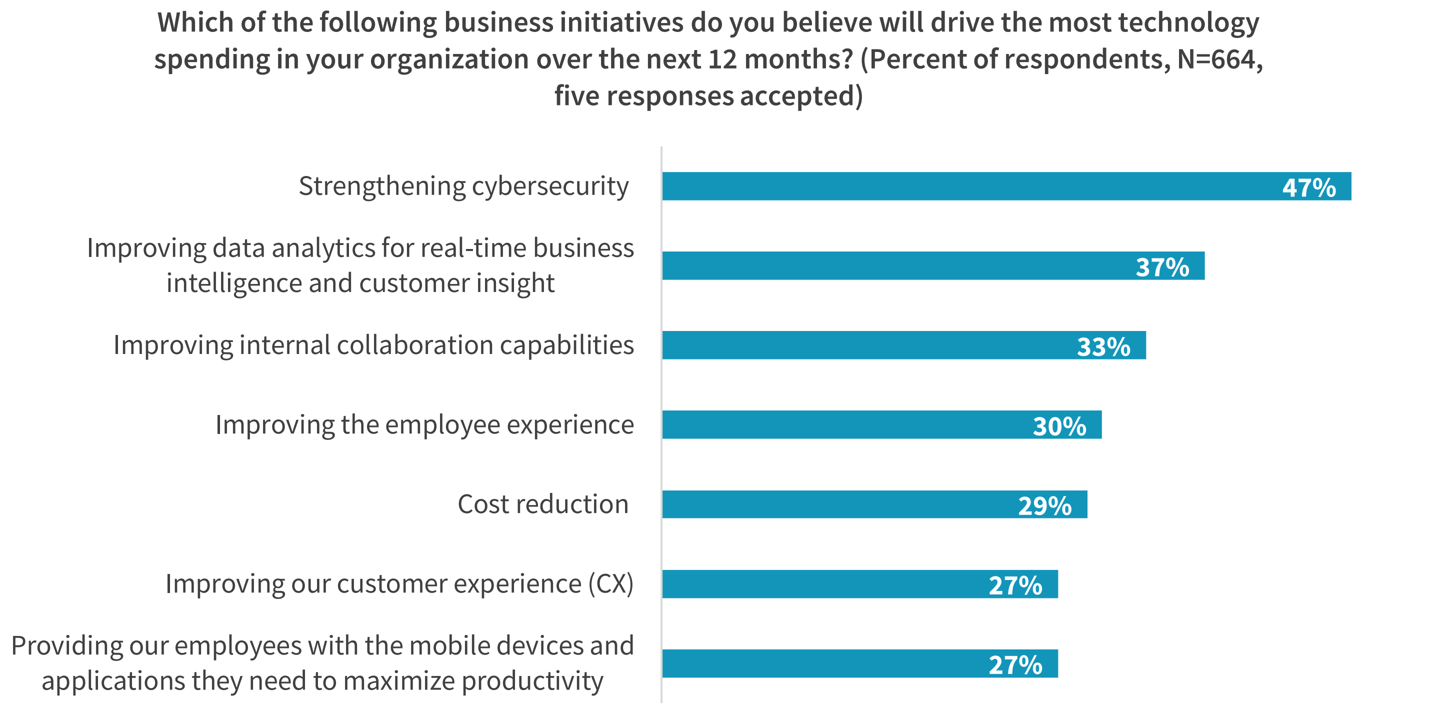
Challenges

According to ESG research, 82% of survey respondents feel cyber-risk is greater than it was two years ago,[1] and 85% of organizations said that threat detection and response was getting harder.[2] These findings are not surprising given the realities of threat detection and response. Multiple security point solutions add complexity from the standpoint of use, management, and support. More solutions capture more data, and more alerts are generated.

The overwhelming number of alerts makes thorough investigation and analysis virtually impossible, delaying detection, response, and remediation. Security and data silos prevent centralized detection and response and inhibit data correlation. Analysts often are assigned to monitor specific areas such as endpoints or networks, and the views, alerts, and traffic analysis occur in isolation from other analysts doing the same tasks. Network and endpoint monitoring tools offer detailed visibility of suspicious activity, but visibility may be low for servers, email traffic, email boxes, and cloud workloads. Lack of visibility and the inability to correlate data across these security layers increase risk significantly.

But security leaders aren't always sure which investments will pay off based on measurable improvements. According to ESG research, when asked which business initiatives will drive the most technology spending in their organizations over the next 12 months, 47% of respondents cited strengthening cybersecurity, making it the most-cited response and 27% cited providing their employees with the mobile devices and applications they need to maximize productivity (see Figure 1).[3]

Figure 1. Top 7 Business Initiatives Driving Technology Spending



Source: Enterprise Strategy Group

[1] Source: ESG Research Report, *Cybersecurity in the C-suite and Boardroom*, March 2021.
[2] Source: ESG Research Insights Report commissioned by Trend Micro, *The XDR Payoff: Better Security Posture,* September 2020.
[3] Source: ESG Research Report, *2021 Technology Spending Intentions Survey*, January 2021.

When security analysts are dealing with these challenges, attackers have an advantage. By investing in XDR, however, organizations can increase analyst effectiveness and efficiency—a sure way to strengthen their cybersecurity postures.

The Solution: Trend Micro Vision One

Extended detection and response builds on learnings from endpoint detection and response (EDR) and analyzes security telemetry from multiple security layers: endpoint, server, cloud workloads, email, and network. XDR helps organizations overcome the limitations of security/data silos, lack of visibility, and alert overload as well as complexities associated with mutiple security and detection solutions. XDR is designed to help organizations suffer fewer attacks, find attacks sooner, and stop them completely.

The purpose-built Trend Micro Vision One platform, which delivers XDR, is deeply integrated into native sensors to present a unified, easy-to-understand view. Distinctive data sources broaden visibility and provide rich context. For example, cloud sources encompass the breadth and timeliness of Linux support, and email sources enhance visibility and response through integration at the application layer. Threat research powers threat analytics and automatic indicator of compromise (IoC) sweeping. Platform apps like XDR Workbench extend detection and response capabilities. XDR Workbench shows all alerts generated, enables alert prioritization based on security scores, displays all assets related to alerts and attacker events, maps events to the MITRE ATT&CK framework, and enables investigation, root cause analysis, and response from the console.

The platform ingests raw telemetry; filters it using techniques such as data stacking, machine learning (ML), rules, and detection models that combine filters; and then identifies attacker tactics, techniques, and correlated events. Correlated detection speeds discovery of both zero-day and targeted attacks. When low-confidence events, behaviors, and actions within or across security layers are correlated, the noise drops significantly. Security teams can more easily and quickly see, understand, and respond to attacks as a result of integrated security analytics and built-in threat intelligence.

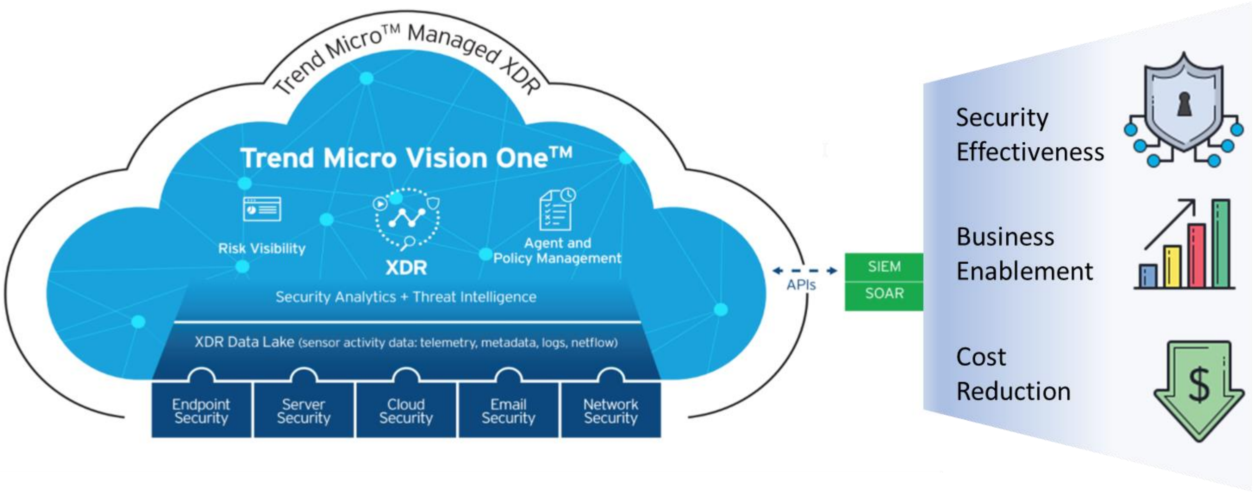
Trend Micro Vision One enables analysts to conduct in-depth guided investigations and choose integrated, contextually aware response actions. Other notable capabilities include:

- Visualizing attacks through an interactive visual representation of events within an endpoint, server, or cloud workload.
- Engaging network analysis capability to replay network communications to see details of command and control communications or lateral movement.
- Mapping techniques to the MITRE ATT&CK framework and linking to related documentation.
- Searching the XDR data lake through all or specific data sources and combining criteria with the MITRE ATT&CK framework.
- Connecting to SIEM and SOAR platforms via APIs.

Simplified views of security posture metrics and trends provide insights into risk. Views include threat alert trends and top endpoints with observed attack techniques.

Trend Micro Vision One can be supported via the Trend Micro Managed XDR service, which leverages all of the capabilities of the platform and provides managed detection and response services for one or more security layers. Managed XDR includes threat hunting; 24x7 monitoring and detection; and rapid investigation, mitigation, and response.

Figure 2. Trend Micro Vision One Platform



ESG Economic Validation

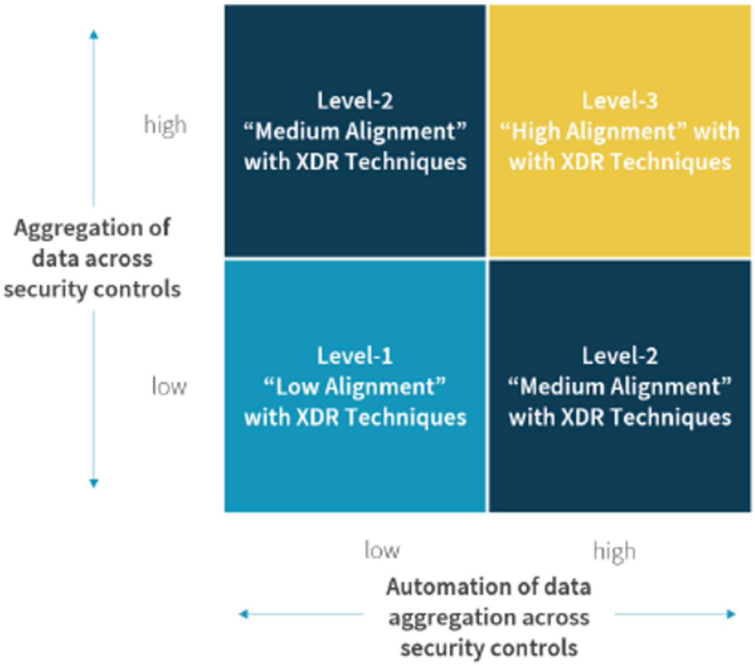
ESG's Economic Validation process is a proven method for understanding, validating, quantifying, and modeling the economic value propositions of a product or solution. The process leverages ESG's custom research; knowledge of the industry, markets, and alternative technologies; expert analyst opinion; and review of third-party or internal testing. ESG conducted in-depth interviews with Trend Micro customers and reviewed customer case studies to better understand and quantify the positive outcomes experienced by organizations using XDR.

Alignment with XDR Leads to Better Overall Security Posture

To validate how alignment with XDR leads to better overall security posture, ESG designed and conducted a survey to assess the value that organizations realize when implementing similar approaches to XDR. Surveyed organizations fell into one of three levels of alignment, with level 3 representing the companies most aligned with XDR techniques. The assessment was based on two dimensions: first, the level of aggregation and correlation across multiple security controls; and second, the level of automation that has been applied to this process (see Figure 3).[4]

[4] Source: ESG Research Insights Report commissioned by Trend Micro, *The XDR Payoff: Better Security Posture*, September 2020.

Figure 3. ESG's XDR Value Assessment Model



Respondents were placed into one of three stages of alignment, based on their responses to 2 questions:

1. How would you describe the information/data in your organization's various security, threat detection, and response controls?

   Siloed ←→ Single source of truth

2. How would you describe the process of integrating and aggregating data from your organization's various security, threat detection, and response controls?

   Manual ←→ Automated

ESG employed this characteristic-based system as a proxy for XDR.

Source: Enterprise Strategy Group

The highest level of XDR alignment occurred in 21% of organizations (see Figure 4),[5] which are already aggregating, correlating, and analyzing data from multiple security controls in a highly automated way.

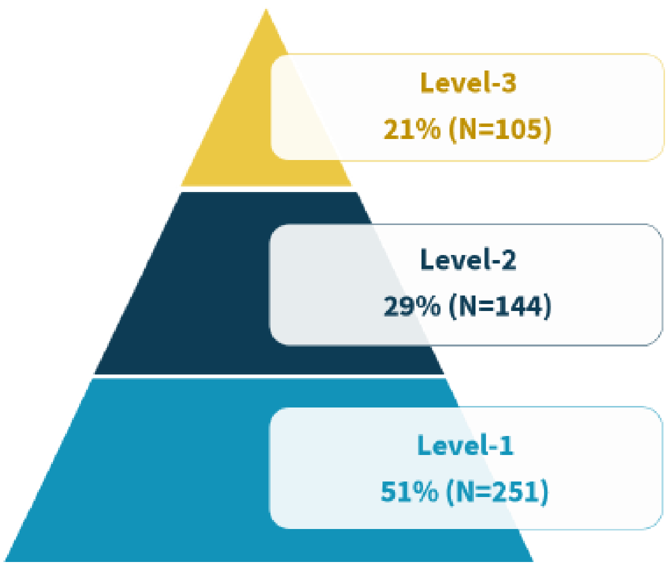
Figure 4. XDR Alignment Maturity Model Distribution

Based on responses, ESG observed the following distribution of organizations. It is important to note the distribution **is consistent across company sizes**:

Level-3 (High Level of Alignment):
- Aggregate data from across controls in an automated way
- 21% of the market today

Level-2 (Medium Level of Alignment):
- Mostly siloed data across security controls with some automated aggregation processes **OR**
- Aggregated data across security controls, but with many manual processes
- 29% of the market today

Level-1 (Low Level of Alignment):
- Mostly/completely siloed data in TDR controls with only manual data aggregation
- 50% of the market today



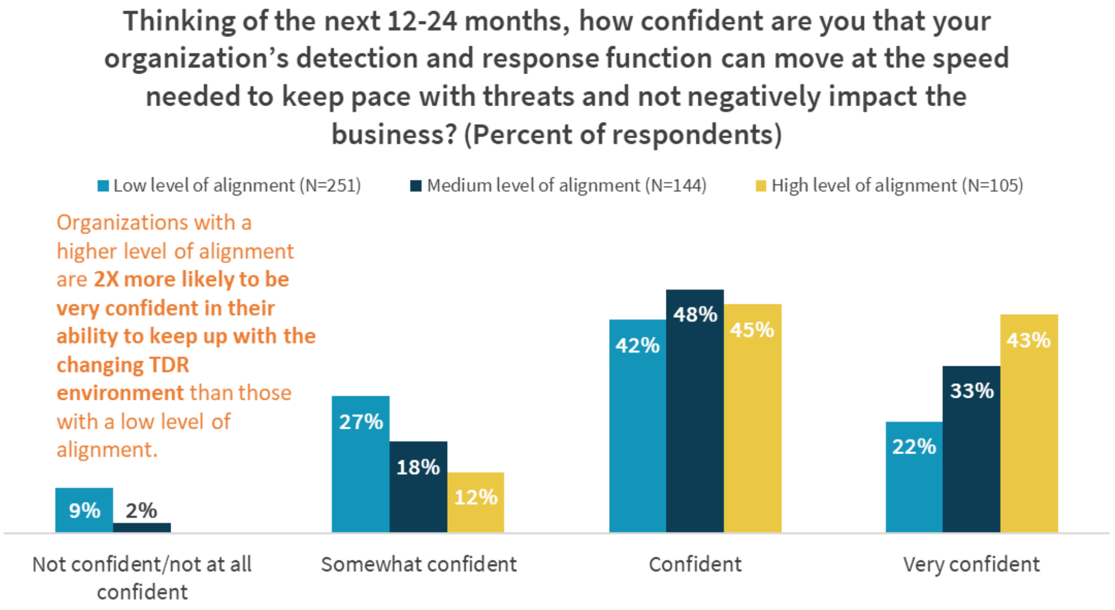
Source: Enterprise Strategy Group

[5] Ibid.

Lower alignment, level-1 organizations are 2.6x more likely than level-3 organizations to describe their detection and response teams as always or often overwhelmed. And while 65% of level-3 organizations with high levels of alignment to XDR report average dwell times of a few days or less, 45% of level-1 lower alignment organizations report dwell times of more than one week. This finding is important because dwell time is a critical metric leading to successful attacks.

Not only do level-3 organizations experience significantly fewer successful attacks, they also reported they were holding their own in the threat detection and response battle and that they were stretched less thin than level-1 and level-2 organizations. ESG found that 88% of organizations with a high level of alignment were confident or very confident that the detection and response function could keep up with threats (see Figure 5).[6]

Figure 5. High Alignment with XDR Results in Greater Confidence in Threat Detection and Response



Source: Enterprise Strategy Group

ESG validated that high alignment with XDR improved overall security posture in three specific areas: better protection, quicker detection, and complete response with less likelihood of repropagation.

Trend Micro Economic Overview

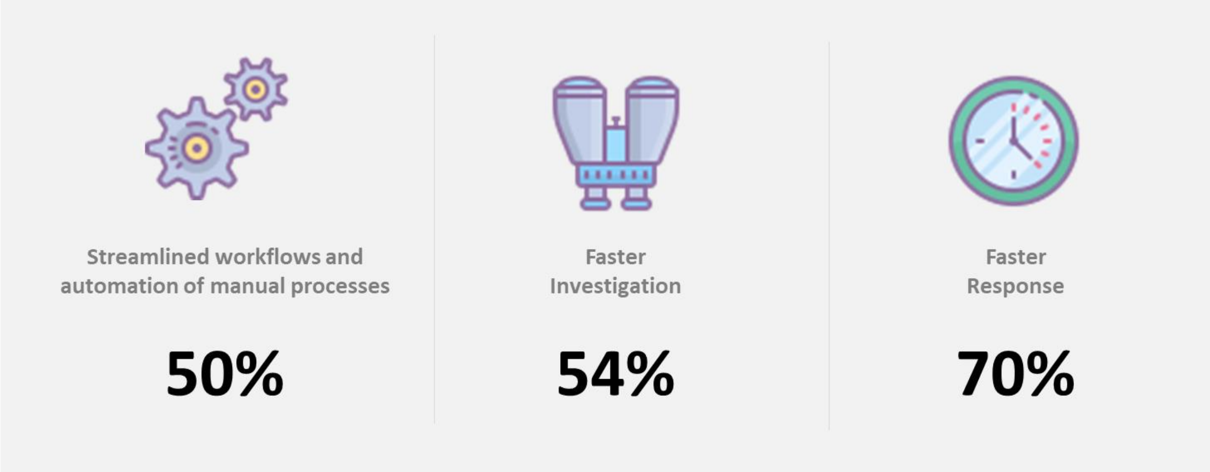
ESG reviewed the Trend Micro Vision One with XDR offering and uncovered economic benefits in the following categories for organizations:

- Security effectiveness – Organizations improved their overall security posture. They experienced a higher level of detection and accelerated mean time to detection with fewer false positives.
- Business enablement – After siloed views and processes were eliminated, organizations were able to streamline, automate, and speed up activities. Smoothly running operations lowered risk and made it easier to take advantage of new opportunities.
- Cost reduction – Savings accrued from vendor consolidation, automation, more efficient triage and investigation, and lower impact of successful attacks.

[6] Ibid.

Our Trend Micro Vision One findings support findings in other ESG research, which showed that organizations with more effective data correlation reported streamlined workflows, faster investigations, and faster response (see Figure 6)[7]—outcomes that also contribute to cost savings.

Figure 6. Effective Threat Data Correlation Produces Operational Improvements



Source: Enterprise Strategy Group

Security Effectiveness

ESG research found that 42% of survey respondents believe there are more cyber-threats today.[8] More threats complicate and intensify detection and response efforts, jeopardizing efficient, rapid remediation. Compared to alternative XDR solutions, the Trend Micro Vision One platform enabled customers to increase security effectiveness and improve their security postures. Reducing complexity was a key reason for overall improvement.

For one customer, lower complexity led to a reduction of more than 25% in human-caused errors. Another stated that two security personnel supported 550 users and 800 devices. Built-in threat intelligence enabled users to search their environments easily.

> ***"XDR tells a story. Not only can I see what is happening, I can quickly find everything that is impacted and immediately take action."***
>
> ***– CISO, healthcare provider***

Customers also reported higher levels of detection, shorter mean times to detection, and fewer false positives—essential contributors to a reduction in security events. A local government customer discussed a ransomware incident that occurred during the decision-making process to strengthen their cybersecurity. "Even though we were not a Trend Micro customer at the time, Trend Micro helped us navigate through the ransomware mess. I am completely confident that we would have been protected from this ransomware attack if we were on Trend Micro XDR at that time."

Trend Micro Vision One, which enables endpoint, email, workload, and network response actions from one place, prompted a customer to comment specifically on the single point of control and the single dashboard to visualize the

[7] Ibid.

[8] Source: ESG Research Report, *Cybersecurity in the C-suite and Boardroom*, March 2021.

threats and the patterns. The single pane of glass and better control were instrumental in allowing the local government customer to now be able to monitor activity and ensure people are using work resources for work—a change that led to better governance planning.

A customer in the hospitality industry described their visibility into email, SharePoint, and Teams, and the ability to make sure that proprietary data was not being passed. Assurances could be made to organizational leaders that their data was secure.

"The reduction in complexity has led to a reduction in human-caused errors of over 25%. This gives us faster detection and remediation." — VP/CISO, medical supplies and services company

A CISO with a medical company confirmed that it was easier for his team to explain the attack and go through the sequence of events saying, "It's like reading a book…easier to digest." An educational institution's security team using managed XDR observed that nearly 60 million events were distilled to approximately 11,000 high-severity events, resulting in "massive value."

With respect to one of the most crucial aspects of security effectiveness—accurate, early detection—customers report their organizations were 2.2 times more likely to detect a data breach or successful attack in a few days or less compared to weeks or months for those without XDR.

Business Enablement

Trend Micro Vision One eliminated siloed views and processes, enabling data consolidation, speeding correlation, and improving mean time to response. The combination of visibility, speed of detection and response, and less noise produced a range of positive outcomes, including lowering the barriers to acting on new opportunities and decreasing the risk involved.

"XDR has given us the confidence to open up portals that have allowed us to navigate the challenges of COVID and quickly expand outside our traditional office."

—Cybersecurity Administrator, local government agency

A cybersecurity director confirmed that visibility into endpoints not on the physical network was a game changer. Now he can look at any employee's machine remotely, search for malware, or even lock down USB ports, all from the cloud. Further, the organization could expand quickly outside of their traditional offices.

Customers conducted day-to-day business more confidently knowing that Trend Micro Vision One was monitoring their email for triggers that the platform analytics correlated with other events to detect phishing attacks or compromised email accounts.

Customers also were able to accelerate the pace of innovation. They relied on Trend Micro Vision One to support digital transformation and diverse workloads across endpoints, servers, virtual machines, multi-cloud, and containers. Given that 33% of organizations surveyed in an ESG research study reported that the deployment of more assets expanded the attack surface,[9] XDR paved the way for customers to undertake business expansion more confidently.

[9] Source: ESG Research Report, *Cybersecurity in the C-suite and Boardroom*, March 2021.

Cost Reduction

Organizations using Trend Micro Vision One lowered costs on several fronts. Consolidating to a single platform from a single vendor eliminated separate offerings from multiple vendors. Automation led to needing fewer people to manage detection and response. For example, the automated, cross-layer detection models of Trend Micro Vision One tied together low-level events in near-real time compared to manual correlation efforts. With fewer false positives to triage, IT/security teams lowered the number of hours needed for alert triaging, individual investigations, and threat hunting. Trend ESG research has found that organizations reported an average of eight FTEs would be needed to replace the aggregation, correlation, and analytics that XDR provides.[10]

> ***"I estimate it would be 5x to 6x more expensive if we tried to use our own employees and less effective at the same time."***
>
> ***—Cybersecurity Administrator, local government agency***

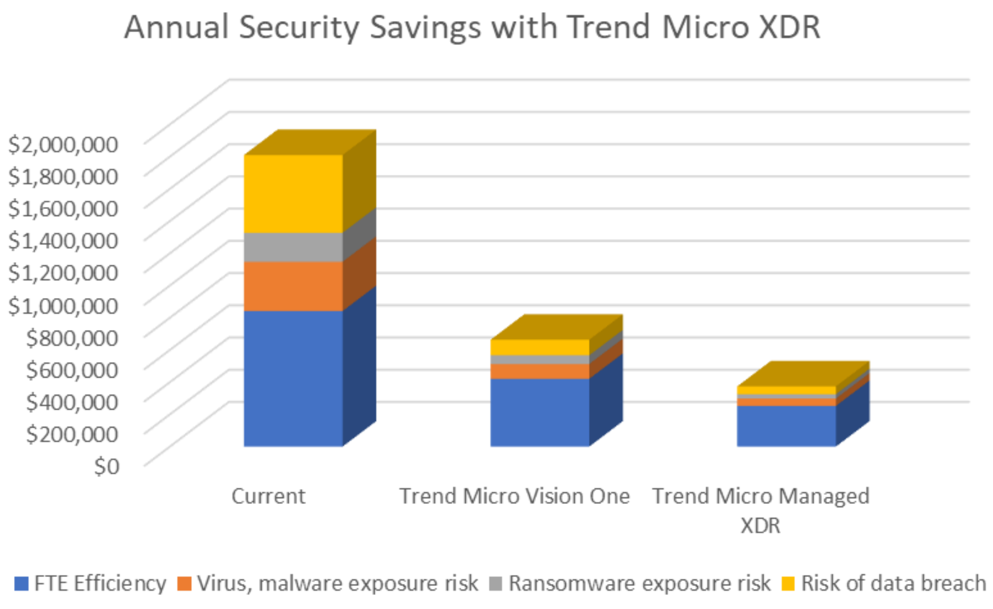
Customers also praised Trend Micro Vision One for lowering the business impacts, risk, and cost of a successful attack. One customer reported that the cost of Trend Micro's XDR expertise is a drop in the bucket of what they would need to pay FTEs to get the same type of visibility into incidents. Another customer reported that without XDR, at least two more people would be needed.

> ***"Our overall product spend has gone down almost 50% when you look at all of the products that Trend Micro has replaced."***
>
> ***— CISO, hospitality industry***

Additionally, Trend Micro Vision One enables organizations to reduce spending on products, due in part to the platform's ability to go beyond EDR and SIEM capabilities and to broaden coverage to numerous operating system versions and multiple security layers.

The CISO of a healthcare organization reinforced the value of Trend Micro by stating, "Lower cost is great, but if cost were not a concern, we still would choose Trend Micro XDR as our solution."

ESG created an economic model using a company with 2,000 employees accessing 3,400 devices and found that organizations save 63% when comparing ad-hoc systems with Trend Micro Vision One. That number jumps to a 79% savings by adding Trend Micro Managed XDR. The categories of FTE efficiency, virus & malware exposure, ransomware exposure, and risk of data breach were considered in this model.



[10] Ibid.

The Bigger Truth

Organizations need to do more to improve their security postures and thwart the onslaught of cyber-attacks. XDR can help security analysts do their jobs more productively by enabling a higher level of detection, faster mean time to detection, fewer false positives, and fewer security events.

Trend Micro Vision One surpasses the limited scopes of EDR, can complement SIEMs, and augments security operations centers (SOCs) with XDR capabilities that connect discrete pieces of malicious activity so analysts can understand the full attack path without having to build the story themselves.

The Trend Micro add-on for Splunk is just one example of Trend Micro's growing API integration portfolio to SIEM and SOAR and third-party infrastructure partners to fit within existing workflows and add more functionality and XDR value.

Research indicates that organizations highly aligned with XDR report better overall security postures in terms of fewer successful attacks, earlier detection, and more complete remediation. ESG validated specific outcomes that users experienced with Vision One through custom research, review of third-party/internal testing, review of customer case studies, interviews of Trend Micro customers, and conversations with industry analysts. The key findings centered on improvements in security effectiveness, business enablement, and cost savings.

ESG strongly recommends consideration of Trend Micro Vision One for next-level enterprise-wide detection and response. Adoption can be phased, although there are clear benefits to subscribing immediately for all security layers. If choices need to be made, email is a good starting point because it is a highly targeted security layer and the entry point for many attacks that turn into breaches. Cloud and server workloads are another top priority for obvious reasons given digital transformation, cloud migration, and work-from-home initiatives.

Given that the top factors for justifying IT investments are cybersecurity and productivity, we believe that Trend Micro Vision One is a two-for-one solution that should rise quickly to the top of an evaluation process.

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