Enterprise Strategy Group™ by TechTarget

WIRTSCHAFTLICHE VALIDIERUNG

Analyse der wirtschaftlichen Vorteile von Trend Vision One

Minimieren Sie Cyberrisiken, beschleunigen Sie Ihre Erkennung und Reaktion und verbessern Sie die allgemeine betriebliche Effizienz mit einer bewährten Plattform für Cybersicherheit

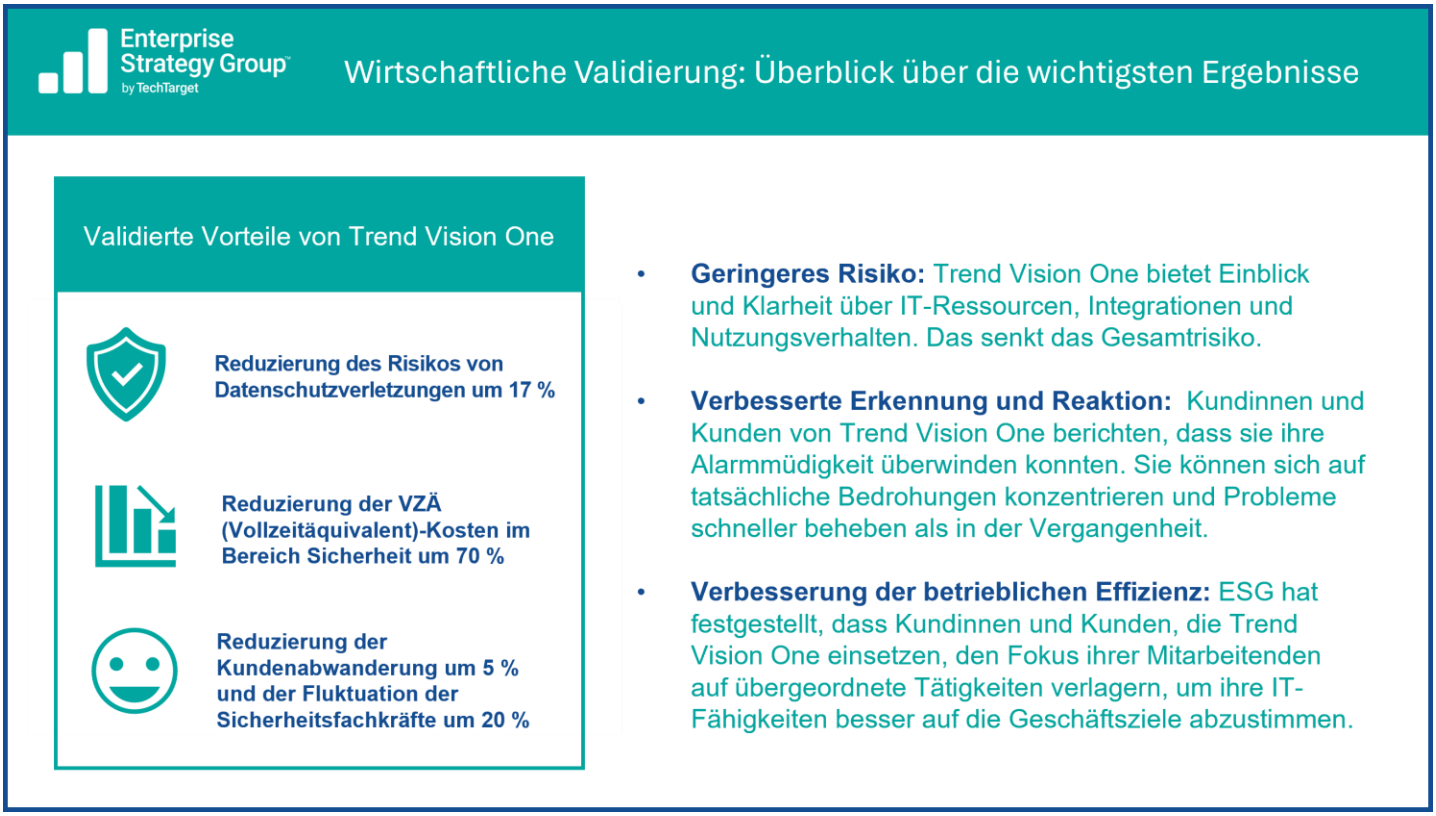
Von Nathan McAfee, Senior Economic Analyst
Enterprise Strategy Group

Januar 2024

Diese wirtschaftliche Validierung der Enterprise Strategy Group wurde von Trend Micro in Auftrag gegeben und wird unter Lizenz von TechTarget, Inc. vertrieben.

Inhalt

Einleitung **3**
Herausforderungen 3
Die Lösung: Trend Vision One 4
Wirtschaftliche Validierung der Enterprise Strategy Group **5**
Trend Vision One: wirtschaftlicher Überblick 5
Geringeres Risiko 5
Verbesserte Erkennung und Reaktion 7
Verbesserung der betrieblichen Effizienz 8
Analyse der Enterprise Strategy Group 10
Fazit **10**



Einleitung

Diese wirtschaftliche Validierung der Enterprise Strategy Group (ESG) von TechTarget konzentriert sich auf die quantitativen und qualitativen Vorteile, die Unternehmen durch den Einsatz von Trend Vision One im Vergleich zu fragmentierten Cybersicherheitsstrategien erwarten können. Ziel ist es, ihre Sicherheitslage zu verbessern und sich vor Sicherheitsbedrohungen und -vorfällen zu schützen, diese zu erkennen und darauf zu reagieren.

Herausforderungen

Der Schutz von digitalen Assets und IT-Ressourcen ist eine Herausforderung, deren Komplexität exponentiell zuzunehmen scheint. Mit jeder Veränderung in der digitalen Landschaft entstehen neue Angriffsvektoren, die es zu erkennen, zu verstehen und zu sichern gilt. ESG hat untersucht, mit welchen Herausforderungen Unternehmen in Bezug auf Cybersicherheit konfrontiert sind. In den meisten Unternehmen und in deren Cybersicherheitsteams stimmen diese offenbar überein:

- **Alarmmüdigkeit.** Cybersicherheitsteams sehen sich oft mit Warnmeldungen konfrontiert, die wöchentlich mehr als 1 Milliarde Protokolle pro 1.000 Geräte generieren. Das schiere Ausmaß der Identifizierung echter Risiken kann die meisten System- und Sicherheitsteams überfordern.
- **Verlagerung des Standorts der IT-Ressourcen.** ESG-Studien haben ergeben, dass in 60 % der Unternehmen unterschiedliche Teams für On-Premises-, Public-Cloud- und Private-Cloud-Ressourcen zuständig sind.[1] Dies führt zu unterschiedlichen Strategien in einem IT-Ökosystem und damit häufig zu kurzsichtigen Entscheidungen und technischen Schulden. Da hybrid arbeitende Belegschaften zur Norm werden, ist die Zahl der zu unterstützenden Standorte stark gewachsen. Mitarbeitende haben jeweils ihren eigenen Standort. Sie arbeiten häufig außerhalb geschützter Unternehmensnetzwerke und auf Hardware, die nicht vom Unternehmen bereitgestellt wurde.
- **Zunehmende Komplexität.** Mit zunehmender Komplexität von IT-Umgebungen steigt die Gefahr, dass die Systeme zur Erkennung, Reaktion, Behebung und Eindämmung von Bedrohungen überlastet und ineffektiv werden. Das Ergebnis ist ein höherer Zeitaufwand für die Erkennung und Behebung von Bedrohungen – und schlimmer noch, eine mangelnde Transparenz der aktiven Risiken. ESG-Studien haben ergeben, dass fast ein Viertel der Unternehmen (23 %) mehr als 25 verschiedene Cybersicherheitsprodukte einsetzt.[2] Dies führt zu digitalen Silos, erhöhter Komplexität und Lücken in der Abdeckung. Damit gehen häufig kurzsichtige Entscheidungen einher, die technische Schulden verursachen.
- **Massives Wachstum bei SaaS-Anwendungen.** Nur wenige Anwendungen sind eigenständig. Da Anwendungen auf APIs, Drittanbietersoftware und mehrere Entwicklungsteams setzen und immer mehr Funktionen in sich vereinen, nimmt die Bedrohungslage für diese Anwendungen zu. ESG-Studien zeigen, dass 76 % der entwickelten Anwendungen mit mehr als 25 APIs verbunden sind, von denen bis zu 75 % mindestens wöchentlich geändert werden.[3] Dies erhöht die Zahl der Angriffsvektoren und zwingt Unternehmen, sich dem Sicherheitsrisiko der über die API verbundenen externen Ressourcen auszusetzen.[4]
- **Risiko unbekannter Ressourcen.** Die Identifizierung aller digitalen Ressourcen ist eine echte Herausforderung. Dies gilt vor allem mit Blick auf die ständigen Anforderungen an den Schutz von Remote-Mitarbeitenden. Ohne einen klaren Überblick darüber, welche Ressourcen die Angriffsfläche des Unternehmens bilden, ist ein Schutz unmöglich.
- **Zunehmende Komplexität von Cyberkriminellen.** Angriffe werden immer raffinierter und immer umfangreicher. ESG hat herausgefunden, dass 68 % der Unternehmen Opfer eines Angriffs geworden sind, der verschlüsselten Datenverkehr verwendet hat, um nicht entdeckt zu werden.[5] Verschlüsselung ist ein Eckpfeiler der Sicherheitsmethodik, aber sie ist nicht mehr die ausfallsichere Präventivmaßnahme, die sie in der Vergangenheit war.

[1] Quelle: Forschungsbericht der Enterprise Strategy Group, *Network Security Trends in Hybrid Cloud Environments*, Juli 2022.
[2] Quelle: Vollständige Ergebnisse der Umfrage der Enterprise Strategy Group, *ESG/ISSA Cybersecurity Process and Technology Survey*, Juni 2022.
[3] Quelle: Forschungsbericht der Enterprise Strategy Group, *Securing the API Attack Surface*, August 2023.
[4] Ebd.
[5] Quelle: Forschungsbericht der Enterprise Strategy Group, *The Evolving Role of Network Detection and Response*, März 2023.

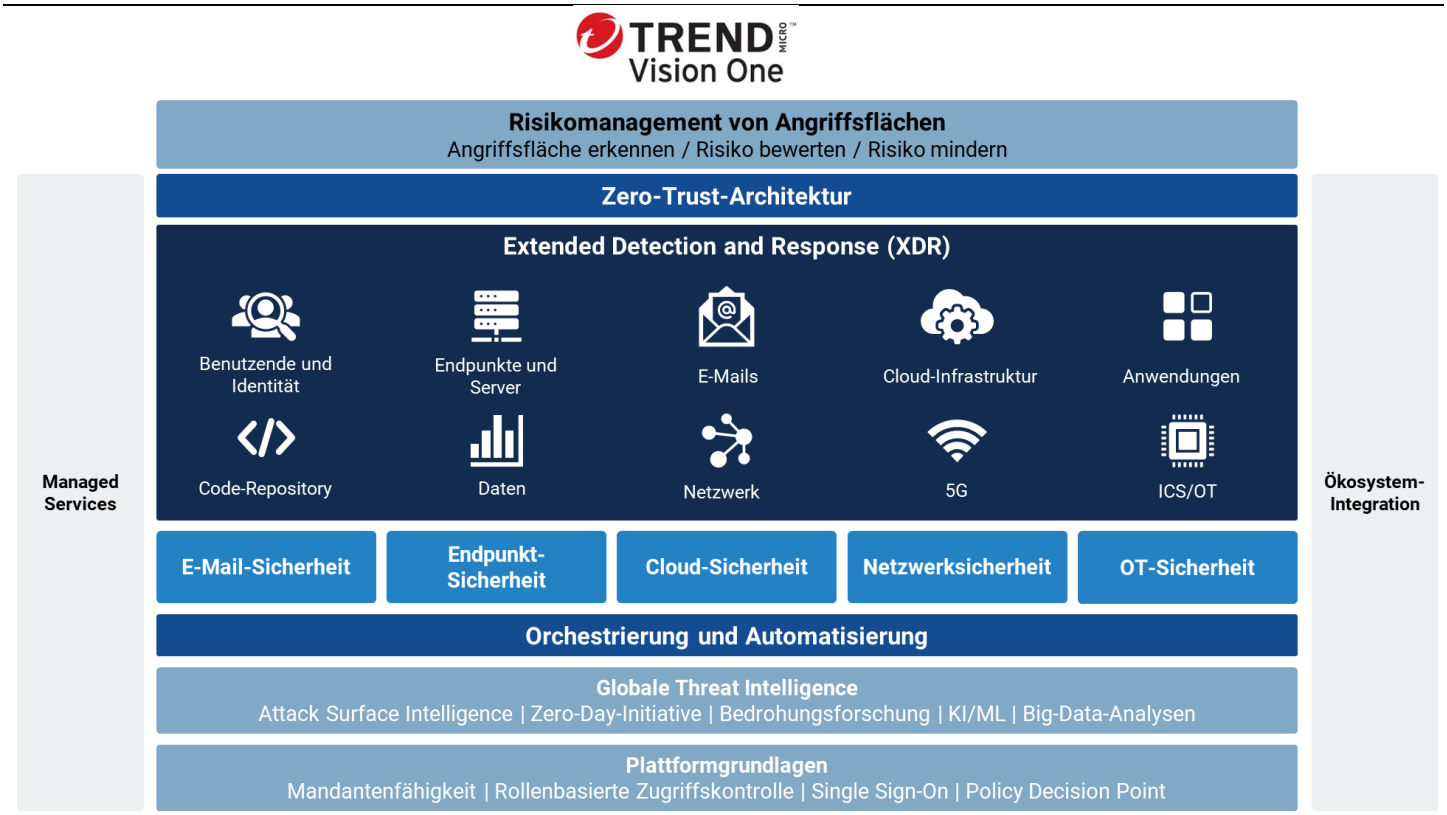
- **Immer schwerwiegendere Folgen von Sicherheitsvorfällen.** Die Auswirkungen von Sicherheitsvorfällen reichen von einfachen Ablenkungen bis hin zu Ransomware-Ereignissen, die durchschnittlich 4,45 Millionen US-Dollar pro Vorfall kosten.[6] Die Daten zeigen, dass Unternehmen, die erfolgreich angegriffen wurden, in den beiden Jahren nach einem Angriff um durchschnittlich 11,9 % schlechtere Leistungen zeigen als der Markt.[7]

Die Herausforderungen sind eindeutig. Die Bedrohungen werden immer zahlreicher und raffinierter. Gleichzeitig gibt es immer mehr Angriffsflächen, da neue Geräte, Cloud-Ressourcen, SaaS-Anwendungen, IP- und Domänenstandorte, Datentypen und vieles mehr hinzukommen. Unternehmen benötigen eine Lösung, die den proaktiven, risikobasierten Schutz und die Bedrohungserkennung in allen Anwendungsfällen vereinfacht.

Die Lösung: Trend Vision One

Wie in Abbildung 1 dargestellt, ist Trend Vision One eine moderne, zweckorientierte, KI-gestützte Plattform für Cybersicherheit. Sie nutzt die kombinierten Möglichkeiten von Lösungen für das Risikomanagement von Angriffsflächen während des gesamten Lebenszyklus, XDR, führende globale Threat Intelligence, KI/ML-Technologie und Zero-Trust-Prinzipien. Ziel ist es, umfassende Funktionalitäten zur Vorhersage, Prävention, Erkennung und Reaktion auf Bedrohungen und damit einen hervorragenden Schutz vor Cyberbedrohungen zu bieten.

Abbildung 1. Trend Vision One kombiniert Prävention, Erkennung, Reaktion und Schutz



Quelle: Trend Vision One

Unternehmen, die Trend Vision One einsetzen, stellen fest, dass sie mit dieser umfassenden Cybersicherheitsplattform mehr proaktive Sicherheit erreichen. Sie können mit der Plattform die Sicherheitsbedrohungen in ihrer gesamten Umgebung besser erkennen, managen und abwehren.

[6] Quelle: IBM Corporation, *Cost of a Data Breach Report 2023*, Juli 2023.
[7] Quelle: Keman Huang et al., *Harvard Business Review*, „The Devastating Business Impacts of a Cyber Breach“, 4. Mai 2023.

Wirtschaftliche Validierung der Enterprise Strategy Group

Die Enterprise Strategy Group (ESG) hat eine quantitative wirtschaftliche Analyse der Auswirkungen durchgeführt, die Trend Vision One auf die Fähigkeit eines Unternehmens haben kann, seine IT- und Geschäftsziele zu erreichen.

Der Prozess von ESG zur wirtschaftlichen Validierung ist eine bewährte Methode. Damit lassen sich die wirtschaftlichen Leistungsversprechen eines Produkts oder einer Lösung verstehen, validieren, quantifizieren und modellieren. Für den Prozess werden die Kernkompetenzen von ESG in den Bereichen Markt- und Branchenanalyse, zukunftsorientierte Forschung sowie technische und wirtschaftliche Validierung genutzt. ESG hat ausführliche Interviews mit Endbenutzenden durchgeführt. Ziel war es, besser zu verstehen und zu quantifizieren, wie Trend Vision One sich auf ihre Unternehmen ausgewirkt hat, insbesondere im Vergleich zu zuvor eingesetzten und/oder ihnen vertrauten Lösungen. Die qualitativen und quantitativen Ergebnisse dienten als Grundlage für ein einfaches Wirtschaftsmodell, bei dem die erwarteten Kosten für die Sicherheits- und Vorfallsinfrastruktur von Trend Vision One mit traditionellen lokalen und Cloud-basierten Diensten verglichen wurden.

Trend Vision One: wirtschaftlicher Überblick

Die wirtschaftliche Analyse durch ESG hat ergeben, dass Trend Vision One seiner Kundschaft erhebliche Einsparungen und Vorteile in den folgenden Kategorien bietet:

- **Geringeres Risiko.** ESG hat festgestellt, dass die Wahrscheinlichkeit von Ransomware-Angriffen und Sicherheitsverletzungen sank und die Auswirkungen tatsächlicher Vorfälle geringer waren.
- **Erkennung und Reaktion auf Bedrohungen.** Die Kundschaft gab an, dass sie mit Trend Vision One deutlich besser in der Lage ist, Probleme zu erkennen, die das höchste Risiko darstellen, und diese Probleme schneller beheben kann.
- **Verbesserung der betrieblichen Effizienz.** Kundinnen und Kunden von Trend Vision One haben festgestellt, dass die Gesamtausgaben für Sicherheit und die Reaktion auf Vorfälle im Vergleich zu früheren Lösungen gesunken sind.

Geringeres Risiko

Der wichtigste Maßstab für jede Sicherheitsplattform ist ihre Fähigkeit, ein IT-Ökosystem zu schützen. ESG-Analysten haben die Umgebungen von Unternehmen vor und nach der Implementierung von Trend Vision One untersucht. Zusätzlich zu direkt miteinander vergleichbaren Kennzahlen hat ESG eine ganze Gruppe neuer Messgrößen gefunden, die Kundinnen und Kunden von Trend Vision One berücksichtigen sollten. Mit Trend Vision One waren Kundinnen und Kunden in der Lage, ganze Klassen digitaler Ressourcen proaktiv zu schützen, die in der Vergangenheit nur unzureichend oder gar nicht geschützt waren. Dazu gehören Geräte, Server, Domain- und IP-Adressen, Cloud-Ressourcen und APIs. Darüber hinaus nannten die für diese Analyse befragten Kundinnen und Kunden Vorteile im Zusammenhang mit der Reduzierung von Risiken, darunter:

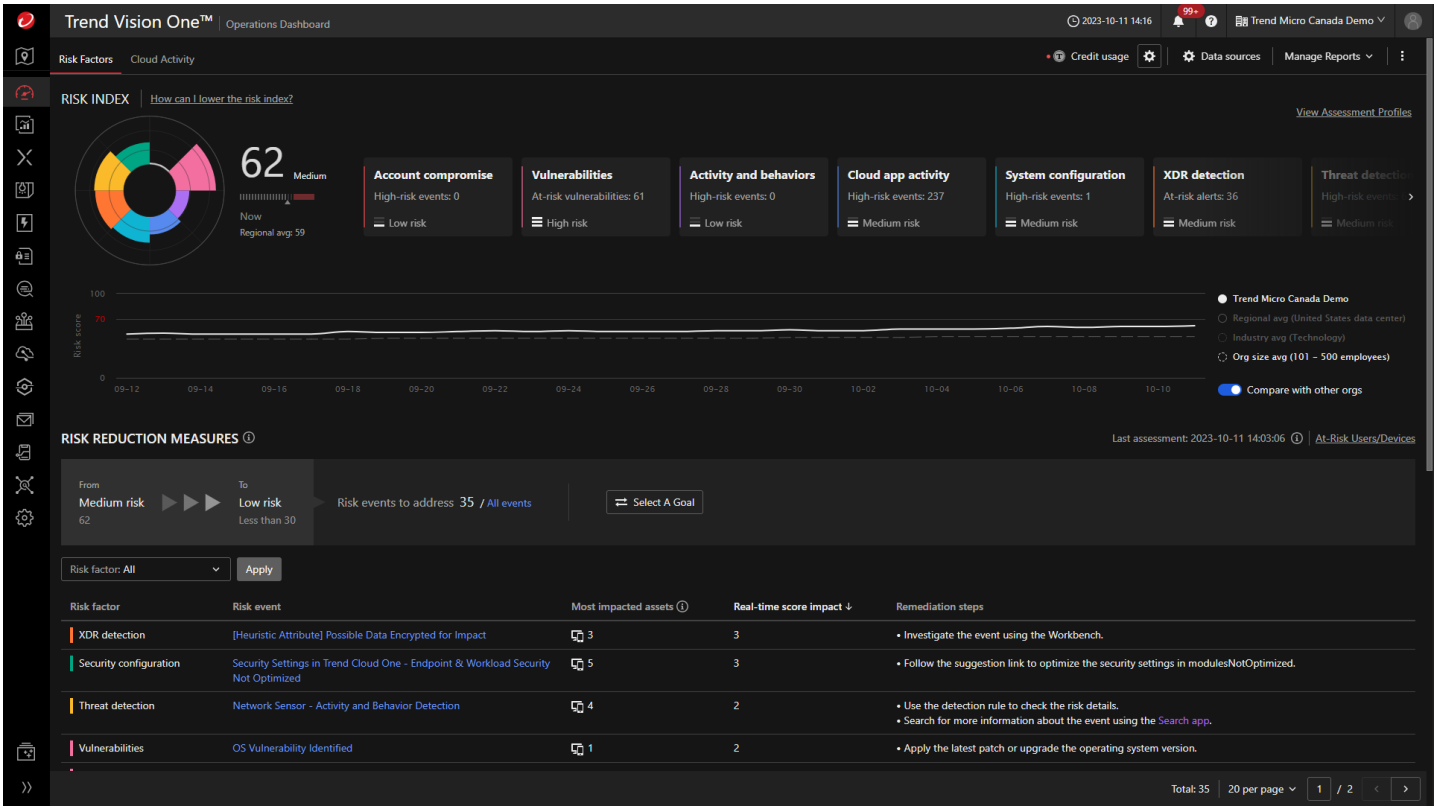
> **„Vision One war kein Ersatz für alte Funktionen. Es ermöglicht uns, Dinge zu sehen, die wir mit unserer alten Lösung gar nicht wahrgenommen haben. Wir scannen und beheben Bedrohungen, die wir in der Vergangenheit erst viel zu spät gesehen hätten.“**
>
> – Sicherheitsmanagement, State Library Systems

- **Geringere Wahrscheinlichkeit von Sicherheitsverletzungen.** Wie bereits erwähnt, schätzt eine der wichtigsten Studien zur Quantifizierung von Risiken die durchschnittlichen Kosten einer Sicherheitsverletzung auf 4,45 Millionen US-Dollar. Im Finanzmodell von ESG wurden als Risiko einer Sicherheitsverletzung 11 % jährlich angesetzt. Auf der Grundlage von Kundenbefragungen konnte dieses jährliche Risiko mit Trend Vision One auf 8 % gesenkt werden. Das führte zu einem jährlichen Nutzen von 1,30 Millionen US-Dollar aufgrund einer verringerten Risikoexposition. Auf die Frage, warum sie der Meinung waren, dass ihre Risikoexposition mit Trend Vision One geringer war, nannten alle Befragten eine verbesserte Transparenz, eine verbesserte Warngenauigkeit und eine kürzere Verweildauer. Letztere war im Vergleich zu ihrer vorherigen Umgebung um durchschnittlich 65 % kürzer. Eine befragte Person meinte, dass der Fokus bei den Auswirkungen einer Sicherheitsverletzung weit über die Kostenkennzahlen hinausgehen sollte: *„Ein Sicherheitsproblem wirkt sich negativ auf unseren Ruf aus. Zahlen sind wichtig, aber das echte Risiko besteht darin, wie unsere Kundschaft uns und unser Engagement für Sicherheit sieht.“*

- **Bessere Transparenz, besserer Einblick.** In jedem Gespräch, das ESG mit Kundinnen und Kunden über die Auswirkungen von Trend Vision One geführt hat, wurde als einer der Hauptvorteile die verbesserte Transparenz ihrer gesamten Sicherheitslage genannt. Angeführt wurde außerdem die neu entdeckte Fähigkeit, Risiken proaktiv zu managen. Diese Transparenz und Risikoverfolgung dient als zentrale Quelle, um eine einheitliche Sicherheitslage für alle Arten von Ressourcen zu gewährleisten. Kundeninterviews ergaben ein einheitliches Bild: *„Vor Trend Vision One wussten wir das einfach nicht.“* Und mit Trend Vision One wurden in der Tat zahlreiche unüberwachte oder sogar unbekannte Ressourcen im Netzwerk festgestellt. Eine weitere Funktionalität von Trend Vision One, die ausdrücklich als bahnbrechend bezeichnet wurde, ist das Betriebs-Dashboard (siehe Abbildung 2). Dieses Feature bietet einen umfassenden Überblick über den Sicherheitszustand und die Risiken in Bezug auf Geräte und Konten eines Unternehmens. Es ermöglicht, in jedem Bereich nach spezifischen Details zu suchen. Das Betriebs-Dashboard von Trend Vision One bietet daher eine konsolidierte Liste von Möglichkeiten zur Verbesserung der allgemeinen Sicherheitslage des Unternehmens.

> **„Das Betriebs-Dashboard von Trend Vision One zeigt uns unser aktuelles Risikoniveau, außerdem detaillierte Möglichkeiten zur Verbesserung unseres Ergebnisses und zur Stärkung unserer Sicherheitslage. Wir könnten es uns nicht leisten, Fachleute einzustellen, die uns diese Art von Einblick gewähren. Aber genau dies ist Teil von Trend Vision One.“**
>
> – Systemadministration, staatliche Behörde der USA

Abbildung 2. Betriebs-Dashboard bietet Risiko-Score und Einblicke für Verbesserungen



Quelle: Trend Vision One

- **Schnelleres Patching.** Bei hybrid arbeitenden Belegschaften befinden sich viele IT-Ressourcen außerhalb der Kontrolle von Update-Systemen des Unternehmens. Die Befragten berichten, dass Trend Vision One ihrer Patch-Strategie mehr Proaktivität, Klarheit und Einfachheit verliehen hat. Dafür sorgte die Nutzung von virtuellem Patching, das auf Threat Intelligence basiert. Eine Aussage lautete: *„Wir haben unser Patch-Management erheblich simplifiziert. Wir haben jetzt Klarheit über die Abdeckung mit Patches und stellen sie 102 Tage schneller bereit als in der Vergangenheit.“*
- **Abstimmung mit wichtigen Compliance-Frameworks.** Unternehmen, die in Compliance-basierten Branchen tätig sind, stellen fest, dass sie mit Trend Vision One in der Lage sind, die Richtlinien besser einzuhalten und den Compliance-Status ständig zu überwachen. Eine befragte Person gab an, dass das Bußgeldrisiko ihres Unternehmens mit Trend Vision One um 60 % gesunken sei. Im Finanzmodell von ESG entspricht diese Reduktion um 60 % einer Risikominderung von 1,2 Millionen US-Dollar pro Jahr.

- **Schutz von Drittanbieter-Integrationen.** Jede Drittanbieter-Integration birgt Risiken, da das Unternehmen die Risiken übernehmen muss, die mit dem Code des Drittanbietenden verbundenen sind. Bei der Untersuchung der Auswirkungen von APIs und Drittanbieter-Integrationen sagte eine befragte Person: *„Die Drittanbieter-Integration von Trend Vision One ist fantastisch. Wir integrieren häufig Sicherheitskomponenten anderer Anbieter. Trend Vision One erstellt externe dynamische Listen. Wird ein verdächtiges Objekt erkannt, wird es automatisch in unsere Firewall eingespeist, um die Bedrohung abzuwehren. Die Transparenz, die wir bei Drittanbieter-Integrationen haben, ist ein entscheidender Faktor. Er ermöglicht uns, auf geschäftliche Anfragen mit ‚Ja‘ statt mit ‚Nein‘ zu reagieren.“* Alle befragten Unternehmen gaben an, dass sie die Funktionen von Drittanbieter-Integrationen eher nutzen würden, insbesondere weil ihnen Trend Vision One Einblick und Schutz bietet.

Verbesserte Erkennung und Reaktion

„Seit der Einführung von Trend Vision One sind wir sicherer. In unserer Machbarkeitsstudie sahen wir eine große Anzahl von Fehlalarmen bei den Alternativen, die wir in Betracht gezogen hatten. Bei Trend Vision One stellen wir fest, dass die erkannten Bedrohungen viel genauer und die Informationen viel spezifischer sind als bei den Lösungen der Mitbewerber.“

– Infrastrukturmanagement, US-Hausbauunternehmen

Bei Millionen von täglich erstellten Protokollen und Tausenden von möglichen Warnmeldungen ist der Versuch, die wichtigsten Bedrohungen zu identifizieren, eine überwältigende Aufgabe. ESG hat Kundinnen und Kunden befragt, um ihre Erkennungs- und Reaktionskennzahlen vor und nach der Einführung von Trend Vision One zu ermitteln. Wie aus Tabelle 1 hervorgeht, hatte Trend Vision One erhebliche Auswirkungen, da die Lösung Störungen reduziert und Unternehmen sich deshalb auf ihre Arbeit konzentrieren können. Darüber hinaus stellten die Unternehmen fest, dass sie Warnmeldungen von Ressourcen erhielten, die ihnen in der Vergangenheit völlig unbekannt waren.

Tabelle 1. Vergleich von Kennzahlen zur Erkennung, Sichtung, Untersuchung und Behebung

	Vor Trend Vision One	Nach Trend Vision One
Anzahl der Warnmeldungen pro Tag	1.000	4
Zeit für Erkennung (Minuten)	11.520	1
Zeit für Sichtung (Minuten)	480	weniger als 1
Zeit für Untersuchung (Minuten)	360	90
Zeit für Behebung (Minuten)	1.860	6
Benötigte VZÄ	5,6	weniger als 1

Quelle: Enterprise Strategy Group, ein Geschäftsbereich von TechTarget, Inc.

„Wir haben die Zeit für die Suche nach Problemen um über 75 % reduziert. Jetzt arbeiten wir schneller und reagieren zügiger auf Bedrohungen. Allerdings ist unsere alte Umgebung damit nicht vergleichbar. Mit Trend Vision One finden und beheben wir Bedrohungen, die wir in der Vergangenheit gar nicht sehen oder verstehen konnten.“
– Leitung Informationssicherheit, Universitätenverbund in den USA

Verbesserung der betrieblichen Effizienz

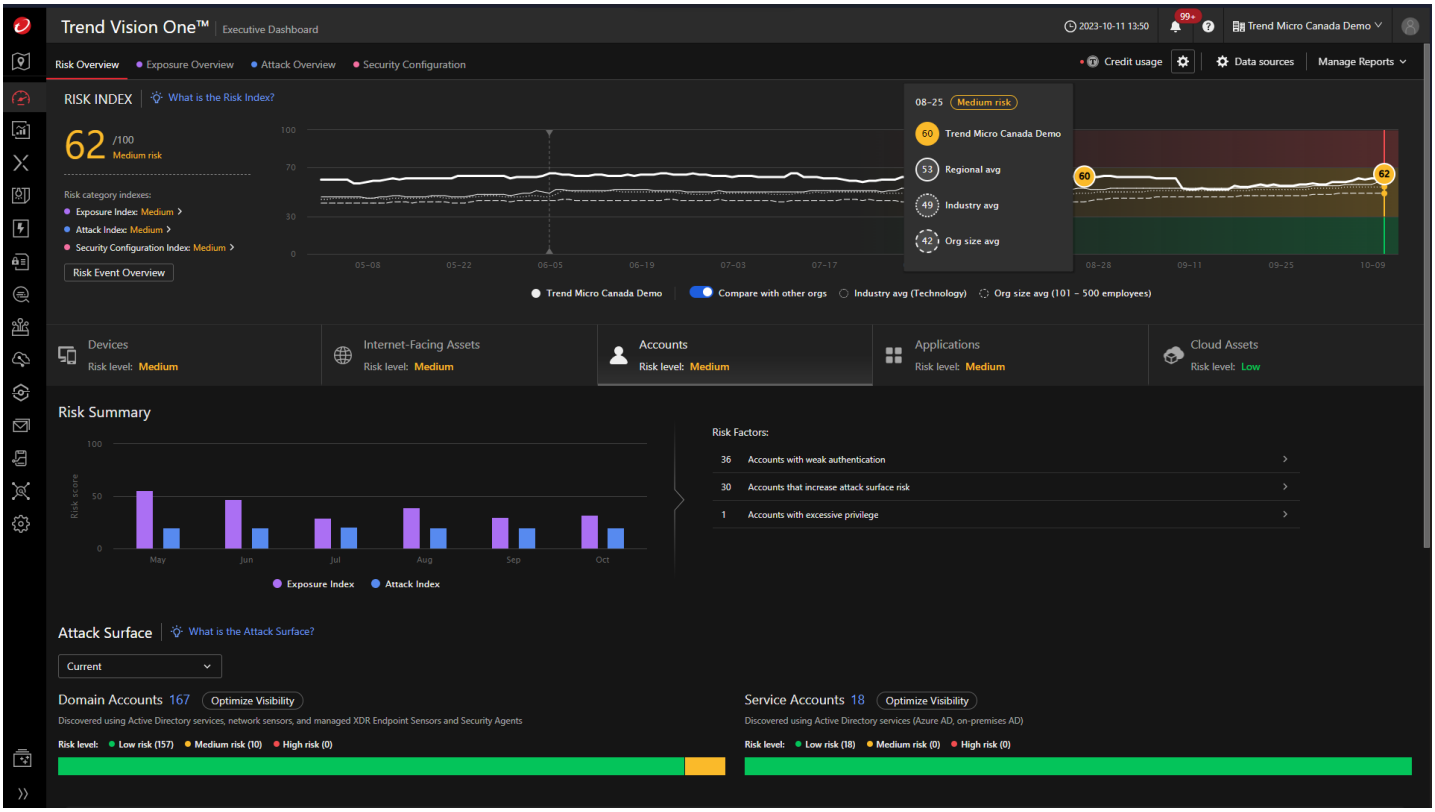
Alle Unternehmen stehen vor der Herausforderung, mit jedem ausgegebenen Dollar so viel wie möglich zu erzielen. Mit Trend Vision One konnten Cybersicherheits- und IT-Teams durch einen plattformbasierten Sicherheitsansatz proaktiver vorgehen. Dies ermöglichte Vorteile in den folgenden Bereichen:

- **Verbesserte VZÄ-Effizienz.** Die befragten Unternehmen gaben an, dass der Personalbedarf für ihre Cybersicherheitsplattform mit Trend Vision One im Durchschnitt um 70 % niedriger war. Ein Unternehmen teilte mit: *„Früher brauchten wir acht Sicherheitsanalystinnen und -analysten, um ein weitaus geringeres Schutzniveau zu erreichen als das, was uns heute dank Trend Vision One mit zwei Personen möglich ist. Und diese beiden sind jetzt viel besser ausgerüstet.“* Im Wirtschaftsmodell von ESG ergeben sich daraus jährliche Einsparungen in Höhe von 1,04 Millionen US-Dollar. Wenn man das Thema Supportkosten betrachtet, konnte mit Trend Vision One die Anzahl der Mitarbeitenden im Bereich Support von 28 auf 17 reduziert werden. Das führte zu jährlichen Einsparungen von 864.000 US-Dollar.

„Unsere Sicherheitsteams hatten einen ständigen Rückstau neuer Dinge, die in unserem Netzwerk implementiert werden mussten. Allein die Risikobewertungen dafür haben mehr Zeit in Anspruch genommen, als uns zur Verfügung stand. Mit Trend Vision One konnten wir unsere Arbeitsbelastung um 70 % senken. Dadurch haben wir jetzt mehr Zeit, um gemeinsam mit unseren Geschäftsbereichen daran zu arbeiten, ihre Ziele und unsere IT-Fähigkeiten besser aufeinander abzustimmen.“
– Leitung Informationssicherheit, Universitätenverbund in den USA

- **Einblick für das Management.** Trend Vision One verfügt über ein integriertes Executive Dashboard, das CIOs, CISOs, Managerinnen und Managern auf einen Blick eine Übersicht über unternehmensweite Trends und Bedrohungen im Bereich Cyberrisiken liefert. Es bietet ihnen die Möglichkeit, jede einzelne Kennzahl so detailliert zu untersuchen, wie sie es wünschen. Eine befragte Person sagte: *„Das Executive Dashboard ist ein fantastisches Tool, das Führungskräften einen sofortigen Einblick in unseren Zustand gibt. Sie können so viele Details erfahren, wie sie möchten, ohne dass sie nach dem Zufallsprinzip auf eine Mitarbeiterin oder einen Mitarbeiter zugehen müssen. Allein das spart uns jede Woche Stunden und führt zu fundierteren Entscheidungen.“* Wie in Abbildung 3 dargestellt, können die Klarheit und der Einblick, die das Dashboard bietet, an das Niveau und die Bedürfnisse der Geschäftsleitung angepasst werden. Für Führungskräfte im Bereich Cybersicherheit ist es jetzt einfacher geworden, mit nichttechnischen Kolleginnen und Kollegen und der Geschäftsleitung zu kommunizieren.
- **Höhere Kundenzufriedenheit.** Kundinnen und Kunden achten auf Sicherheitsverstöße und schätzen sichere Interaktionen, die gleichzeitig ein reibungsloses Erlebnis für Benutzende bieten. Die Befragten schätzen, dass sie die Abwanderungsrate ihrer Kundinnen und Kunden von 6 % auf 5,7 % reduzieren konnten, insbesondere aufgrund der Schutzmechanismen von Trend Vision One und der Art und Weise, wie Trend Vision One Drittanbieter-Integrationen ermöglicht. Im Wirtschaftsmodell von ESG führt diese Verbesserung der Kundenabwanderung um 0,3 % zu einem jährlichen Nutzen von 2,43 Millionen US-Dollar.

Abbildung 3. Das Executive Dashboard bietet einen aktualisierten Status mit der Möglichkeit, nach Details zu suchen



Quelle: Trend Vision One

- **Höhere Mitarbeiterzufriedenheit.** Die Befragten berichten, dass sich die Zufriedenheit der Mitarbeitenden mit Trend Vision One stark verändert hat. ESG hat zahlreiche Berichte über Mitarbeitende ans Licht gebracht, die mehr Befugnisse haben und weniger Zeit mit alltäglichen Aufgaben verbringen. Sie verlagern ihren Schwerpunkt von untergeordneten Tätigkeiten wie der Überwachung von Protokollen und grundlegender Recherche zu übergeordneten Tätigkeiten, um IT- und betriebliche Probleme zu lösen. Die befragten Unternehmen schätzten, dass die Fluktuation ihrer IT-Mitarbeitenden seit der Einführung von Trend Vision One um mehr als 20 % zurückgegangen ist. Eine befragte Person berichtete: *„Unsere Mitarbeitenden lieben es, in dieser Umgebung zu arbeiten. Wir haben die Flexibilität, ihnen die richtige Herausforderung abhängig von ihren Fähigkeiten zu bieten, und konnten einen Großteil der alltäglichen Aufgaben, die traditionell mit Sicherheitsprodukten verbunden sind, durch einen plattformbasierten Ansatz und KI-gestützte Workflows vollständig eliminieren.“* Das Wirtschaftsmodell von ESG ergab, dass sich dieser Nutzen auf 75.000 US-Dollar jährlich beläuft.
- **Geringere Sicherheitskosten.** Trend Vision One vereint umfassende Cybersicherheitsfunktionen in der gesamten Kundenumgebung auf einer einzigen Plattform. Einige dieser Funktionen ersetzen bestehende, isolierte Einzellösungen, und einige Plattformfunktionen umfassen neue Kategorien von Innovationen, die die allgemeine Sicherheitslage verbessern. Mehrere Unternehmen konnten ihre Produktausgaben senken, und 40 % der befragten Unternehmen gaben an, dass sie jährlich mehr als 500.000 US-Dollar an Cybersicherheitskosten einsparen konnten.
- **Geringerer Aufwand für Audits.** ESG hat festgestellt, dass die Kosten für die Einhaltung von Vorschriften und für Audits erheblich gesenkt werden konnten. Das ESG-Finanzmodell ergab eine jährliche Kostenreduzierung in diesem Bereich in Höhe von 207.000 US-Dollar. Ein Unternehmen gab an: *„Früher waren vier Mitarbeitende nur mit Audits beschäftigt. Mit Trend Vision One braucht es für dieselbe Arbeit nicht einmal eine ganze Arbeitskraft.“*

Analyse der Enterprise Strategy Group

ESG nutzte die von den Anbietenden zur Verfügung gestellten Informationen, öffentliches und branchenspezifisches Wissen über Wirtschaft und Technologien sowie die Ergebnisse von Kundenbefragungen, um ein Drei-Jahres-Modell für TCO/ROI zu erstellen. Das so entstandene Modell vergleicht die Kosten und Vorteile von Trend Vision One mit einem modellierten Beispielunternehmen, das mehrere Produkte zum Schutz vor Cyberangriffen einsetzt. Zur Grundlage des modellierten Szenarios beigetragen haben ESG-Befragungen von kürzlich umgestiegenen Kundinnen und Kunden, außerdem die Erfahrung und Expertise in der wirtschaftlichen Modellierung und der technischen Validierung.

Das von ESG modellierte Unternehmen ist in der Hightech-Branche tätig, beschäftigt 15.000 Mitarbeitende, verfügt über 34.950 Endpunkte und erzielt einen Jahresumsatz von 2,7 Milliarden Dollar. Es hat 8,4 Vollzeitäquivalente (VZÄ), die die Cybersicherheit managen, und 28 Supportanalystinnen und Supportanalysten. Das Unternehmen besitzt international 84 Standorte und wächst um zirka 3 % pro Jahr.

Bedeutung

Alle befragten Kundinnen und Kunden gaben an, dass Trend Vision One nicht nur bestehende Produkte ersetzt hat. Es stellt auch eine neue Plattform mit Funktionalitäten bereit, um bestehende Einzellösungen zu ersetzen und gleichzeitig unzählige neue Fähigkeiten hinzuzufügen. Dank dieser Funktionalitäten konnten die Kundinnen und Kunden ihre Sicherheitslage weit über das in der Vergangenheit Mögliche hinaus proaktiv stärken. ESG hat darauf verzichtet, eine alte (Ist-)Umgebung zu erstellen, in der all diese zusätzlichen Funktionalitäten zu Vergleichszwecken genutzt wurden. Stattdessen wurden wir die Auswirkungen des Umstiegs auf Trend Vision One anhand von kundenspezifischen Szenarien quantifiziert.

Fazit

Die Anzahl und die Raffinesse von Cyberbedrohungen nehmen zu, während die Angriffsflächen durch neue Standorte, Datentypen, Datenquellen und Anwendungsfälle immer größer werden. Die Suche nach einer Cybersicherheitslösung führt bei Unternehmen am Ende allzu oft dazu, dass sie ein Wirrwarr von Produkten haben und dabei entweder Silos oder Lücken entstehen. Dies kann zu einer protektionistischen Haltung führen, die die Geschäftsbereiche zwingt, innerhalb bestimmter Grenzen zu arbeiten, anstatt die IT zur Unterstützung neuer Geschäftsmöglichkeiten zu nutzen. Unternehmen in diesen Szenarien gehen unnötige Risiken ein. Sie stellen fest, dass kurzsichtige Entscheidungen eine ständige Fehlerbehebung erfordern, wodurch technische Schulden entstehen, die einen Teil künftiger IT-Budgets aufzehren. Trend Vision One ist eine Cybersicherheitsplattform, die umfassende Präventions-, Erkennungs- und Reaktionsfunktionen zum Schutz von Benutzenden, Endpunkten, E-Mails, Anwendungen, Netzwerken, Clouds, Infrastruktur und Daten bietet. Trend Vision One stützt sich auf führende globale Threat Intelligence, die nur wenige andere anbieten können. Es unterstützt Sicherheitsanalystinnen und -analysten jedes Erfahrungsniveaus mithilfe von KI, um die Sicherheit effektiver zu erhöhen und Cyberangriffe zu vereiteln.

Die Enterprise Strategy Group (ESG) analysierte die Auswirkungen, die Trend Vision One auf die Fähigkeit eines Unternehmens haben kann, eine Umgebung mit proaktiver und umfassender Cybersicherheit zu schaffen. Im Rahmen dieses Prozesses befragte ESG aktuelle Kundinnen und Kunden von Trend Vision One. Ziel war es, zu verstehen, welche Herausforderungen diese in ihrer bisherigen Cybersicherheitsumgebung hatten und wie sich die Funktionalitäten mit Trend Vision One verändert haben. ESG hat festgestellt, dass die Kundinnen und Kunden in der Lage waren, ihr Risiko zu senken, ihre Erkennungs- und Reaktionsfunktionen zu optimieren und die IT besser auf die geschäftlichen Anforderungen abzustimmen. Sie konnten der Geschäftsleitung Einblick bieten, damit sie fundierte Entscheidungen treffen konnte, ohne die Mitarbeitenden ständig um aktualisierte Informationen bitten zu müssen.

Wenn Ihr Unternehmen nach einer Cybersicherheitsplattform auf Enterprise-Niveau sucht, die es Führungskräften, Managerinnen und Managern, Cybersicherheits- und IT-Teams ermöglicht, Ihre gesamte Umgebung zu verstehen und zu schützen, empfiehlt ESG dringend, sich mit den Funktionalitäten von Trend Vision One auseinanderzusetzen.

Informationen zur Enterprise Strategy Group
Die Enterprise Strategy Group von TechTarget bietet fokussierte und umsetzbare Marktinformationen, Studien zur Nachfrage, Beratung durch Analysten, GTM-Strategieberatung, Lösungsvalidierungen und individuelle Inhalte als Unterstützung beim An- und Verkauf von Unternehmenstechnologien.

contact@esg-global.com
www.esg-global.com