Technical Report

More than a number: your risk score explained

Understanding risk score calculations

January, 2023
Trend Micro

Executive summary

Developing a resilient security posture requires a thorough and holistic understanding of the amount of risk the systems and applications making up your corporate environment face. To quickly and accurately assess this risk, Trend Micro Vision One™ Risk Insights surfaces continuously updated metrics. This distills complex information into easy-to-understand individual asset risk scores, as well as a company-wide risk index.

Trend Micro Vision OneTM constantly monitors cyber assets—devices, public domains and IPs, applications, cloud assets, and identities—by ingesting and analyzing vulnerability, exposure, and existing security control data. In addition, it employs extended detection and response (XDR) telemetry and threat intelligence feeds to develop a dynamic risk score.

This risk score is a function that considers two variables:

1. **the likelihood of a threat actor gaining access to the corporate environment and**
2. **the potential impact of such an event. Using these factors, the platform presents the result as an integer between 0 and 100, representing the overall risk to an organization's assets.**

With dynamic and accurate visibility into risk and your current security posture, your organization can make informed decisions about prioritizing and addressing risk. Furthermore, security analysts can perform manual or automated access control decisions based on your risk score and your organization's unique parameters.

Connected products from your security stack continuously query the platform about an asset's status and its associated risk score, as well as the risk score of the endpoint.

Then, if an event occurs within the parameters of a security risk, the platform can remediate this risk by forcibly signing out or disabling the user entirely. Some organizations can tolerate a certain amount of risk. Quantifying it can enable them to decide whether to accept, mitigate, or avoid the risk entirely and enables security teams to operationalize zero-trust architectures.

NIST SP 800-30 Revision 1 Guide for Conducting Risk Assessments defines risk as a measure of the extent to which an entity is threatened by a potential circumstance or event. It is expressed as a function of the impacts that would arise should the event occur and the likelihood of the event occurring at all. Risks in this context include organizational assets, individuals, other organizations, the nation, and organization operations including mission, functions, image, and even reputation.

Benefits of continuous cyber risk scoring

The zero-trust security model is the practice of removing the implicit trust of any entity. Historically, traditional architectures, devices, and identities could adhere to trust protocols within a corporate LAN or another permissioned or geographically bound network. However, today's complex and dynamic environments span cloud services and infrastructure across geographic zones, including mobile and IoT devices. As a result, every endpoint represents a new boundary where all transactions must be verified. The foundation of a zero-trust model should continuously assess risk while tracking user identity and access. Organizations in search of a solution to this problem need to look no further than Trend MicroTM Zero Trust Secure Access.

Due to this ever-increasing complexity, a zero-trust security model requires continuous and in-depth monitoring. This ensures you have a complete picture of active and potential risks in your modern and dynamic environment. Ideally, threats are mitigated using automated response options before a security operations team (SOC) needs to investigate and more importantly, before a full-scale breach can occur. Trend Micro Vision One continuously recalculates risk scores to thwart attempted breaches at the earliest opportunity.

Analysts can then use the risk scores to gain insight into which areas of the environment require attention. A numerical risk score helps them quickly assign priority to which risks must be addressed first.

Moreover, management and leadership can enable relative comparisons and benchmarks of risk scores as a clear indication as to whether their organization's security posture is improving or declining over time. Furthermore, leadership teams can compare their security posture to peers within the same industry, region, and organization size.

The impact is the criticality of the asset as determined by business value. This value is based on the confidentiality, integrity, and availability (CIA) triad, outlined in NIST SP 800-60. Trend Micro Vision One monitors asset attributes and behavior patterns to assess the business value and represent them as profile tags.

Identifying, estimating, and prioritizing risks

The NIST guide recommends four distinct steps toward a comprehensive risk assessment. The first step is to prepare for the assessment by identifying the purpose, scope, assumptions, constraints, sources of information to be used as inputs, and the risk model and analytic approaches to be employed. The risk model defines the key risk factors and the relationship between them. Risk factors include, but are not limited to, the likelihood and impact, moreover the threat, vulnerability, predisposing condition, and asset business value.

Following preparation, the second step towards risk assessment is to conduct the assessment. This includes identifying relevant threat sources, events that can be produced by those sources, and vulnerabilities that could be exploited through those events. Additionally, this is when the likelihood and adverse impacts are determined.

The third step is to communicate the results of the risk assessment and to share the information to help support other risk management activities. Lastly, the fourth step of the NIST-recommended approach to risk assessment is to continually monitor the identified risk factors and to continually update it using the results from the monitoring set forth by the existing risk assessment.

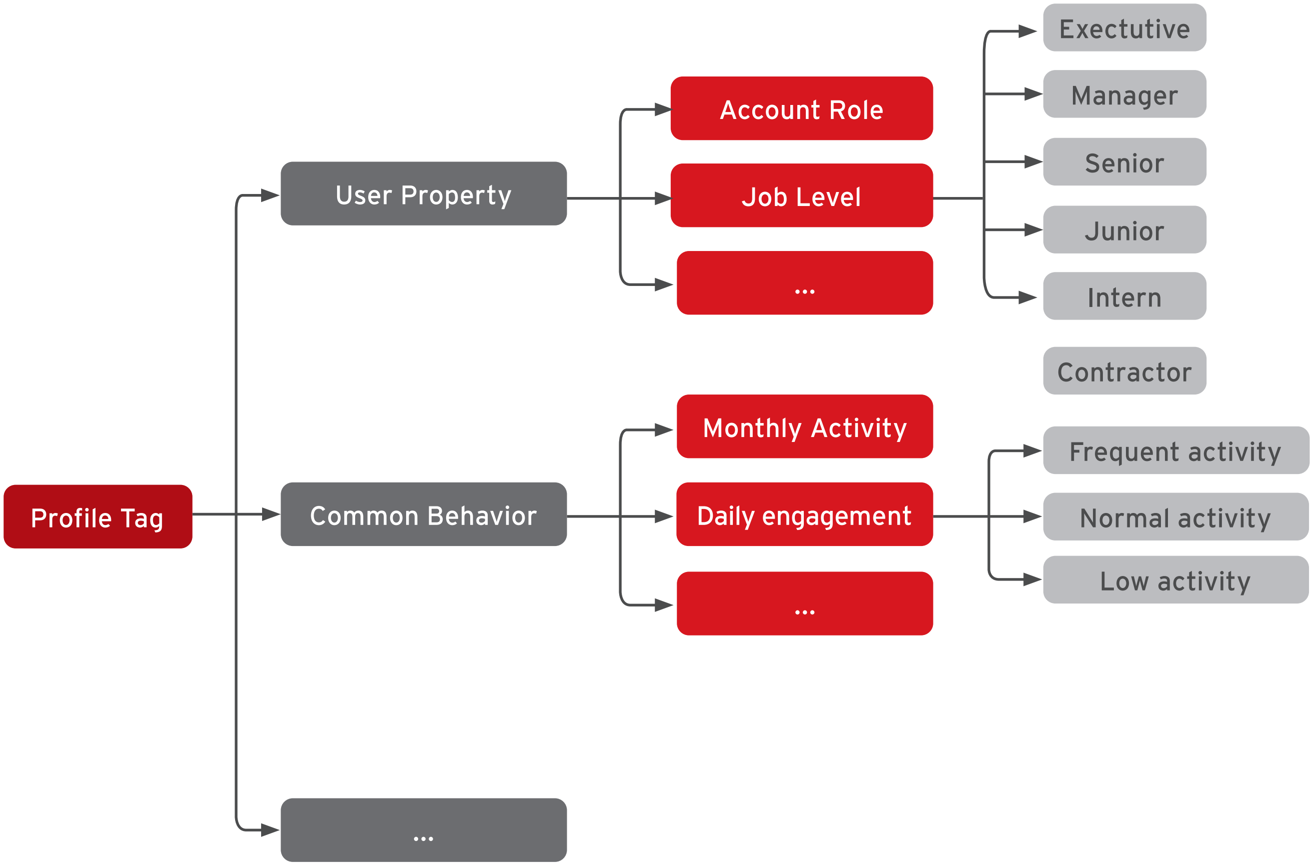
Confidentiality, integrity, and availability

Confidentiality means that data, objects, and resources are protected from unauthorized access. Integrity means that data is protected from unauthorized changes to ensure reliability and correctness. Availability means that authorized users have access to the systems and resources they need. Trend Micro Vision One assesses assets based on attributes and behaviors that affect these three factors.

For example, consider a user's job level. The criticality of an executive team member's account is likely to be higher than an entry-level employee's account. Job function, account status, account privilege, asset type, and device ownership are other asset attributes that affect the CIA triad value.

Similarly, behaviors also affect the CIA triad value. Common behaviors such as monthly activity, daily engagement, and access history are all under consideration when assessing and deriving the CIA triad value for any given asset.

Figure 1: Profile Tags in Attributes and Behaviors



Confidentiality Value Definitions

Value	Level	Description
5	Very High	Contains the most sensitive secrets of the organization, involving the fate of future development, fundamental interests of the organization. If leaked, it will cause catastrophic damage.
4	High	Contains the organization's important secrets, the leakage of which will cause serious damage to the security and interests of the organization.
3	Medium	General secrets of the organization, the disclosure of which could cause damage to the security and interests of the organization.
2	Low	Information that can only be disclosed within the organization or within a department of the organization, the disclosure of which is likely to cause damage to the organization's interests. The dissemination of such information may cause minor damage to the organization's interests.
1	Very Low	Publicly available information, including public information-processing equipment and system resources.

Integrity Value Definitions

Value	Level	Description
5	Very High	The value of integrity is very high, and unauthorized modification or disruption can have a significant or unacceptable impact on the organization.
4	High	High integrity value, unauthorized modifications, or disruptions can have a significant impact on the organization, have a severe business impact, and are more difficult to remediate.
3	Medium	Medium integrity value, unauthorized modification or destruction can have an impact on the organization, and the impact on the business is significant. However, it can be compensated for.
2	Low	Integrity value is low, unauthorized modification or destruction will have a minor impact on the organization, and the impact on the business will be minor, and easy to be remediated.
1	Very Low	Integrity value is very low, unauthorized modification or disruptions have negligible impact on the organization and negligible impact on the business.

Availability Value Definitions

Value	Level	Description
5	Very High	Very high availability value, with an annual availability of information and information systems of more than 99.9% for legitimate users, or the system does not allow disruptions.
4	High	High availability value, where the availability of information and information systems to legitimate users is more than 90% per day, or the system allows for less than 10 minutes of disruption.
3	Medium	Medium availability value, where the availability of information and information systems to legitimate users is at least 70% during normal working time, or the system allows interruption time less than 30 minutes.
2	Low	Low availability value, where the availability of information and information systems to legitimate users is at least 25% during normal working hours, or the system allows interruptions of less than 60 minutes.
1	Very Low	The availability value is negligible, and the availability of information and information systems to legitimate users during normal working time is less than 25%.

Calculating Risk Scores

Trend Micro incorporates an array of factors into the risk score, including the configuration of security controls, asset criticality, vulnerabilities, and threat activity. It then formulates a risk score for each asset type and an index for the whole organization. The result is an integer between 0 to 100 that falls into one of three levels :

Risk Score Levels

Level	Score
Low	0-30
Medium	31-69
High	70-100

This score factors in the asset's attack events, exposure events, and security configuration events and multiplies them by the impact. The attack surface may be small for an asset with low business impact and minimal privileges. Conversely, higher-value assets with a broader scope of privileges make for a greater attack surface. The risk scores are calculated individually for every asset, with each score considering asset type and criticality.

While the risk score calculation is complex, it can be summarily expressed as the geometric mean of the likelihood and the impact—that is—by multiplying the likelihood by the impact and taking the square root of the product:

$$RiskScore = \sqrt{likelihood \times impact}$$

The formula communicates how likelihood is calculated as a weighted risk factor based on probability and how the impact is calculated by evaluating the criticality with measurements of confidentiality, integrity, and availability.

Likelihood

The likelihood that threat events can exploit a weakness in the IT infrastructure—either directly or through a chain of vulnerabilities—is converted to a weighted risk category based on probability.

The likelihood of a threat event is evaluated based on the weighted sums of an individual asset's attack detection, exposure, and security configuration in the following equation, where "P" is a function that considers the likelihood from these three categories as a result in range 0-100. The higher the likelihood, the greater probability of a risk occurrence.

$$likelihood \ = P(attackEvents, exposureEvents, securityConfigurationEvents)$$

The weighted summation of events is the sum of all ***weight x event*** event products for their respective event types, where the sum of the k value is equal to 1.

$$attackEvents = \sum_{k=1}^{x} weight_k \ * score_k$$

$$exposureEvents = \sum_{k=1}^{y} weight_k \ * score_k$$

$$securityConfigurationEvents = \sum_{k=1}^{z} weight_k \ * score_k$$

The platform considers over 800 events in the attack, exposure, and security configuration risk categories and scores each category between 1 and 100, where higher scores indicate more severe security issues and more recent events have greater weights.

Risk categories

- Attack category: Captures threat detections from different security modules, including the security analytics engine, to capture previous and existing threat activity, as well as relevant data to help predict future malicious movement. This categorization contributes to evaluating the likelihood of an attack.
- Exposure category: Represents weaknesses that could be exploited—including vulnerabilities and CVEs, security and cloud misconfigurations, compromised accounts, and abnormal activity from users, devices, and cloud apps.
- Security configuration category: Considers deployed and missing security controls within the environment, including protection products like endpoint protection and specific feature sets like behavioral monitor. When an organization is sufficiently configured, it is better protected and considered less likely to experience an attack.

The attack, exposure, and security configuration weighted sum calculations are represented in the equation below. The events are generated using telemetry from the organization's existing security stack, including Trend Micro solutions, as well as API integrations with SIEM, SOAR, identity access management, firewall, threat intelligence, IT service management, and ticketing products.

Impact

Defined as the magnitude of harm that a breach can be expected to cause, the impact is effectively the attack surface as determined by evaluating the asset's criticality based on confidentiality, integrity, and availability. This is a summarization that considers the overall CIA triad requirements from all the business-related profile tags for this asset.

In practice, the impact is calculated from these three asset requirements, scored from 1 to 5:

$$impact = Q(confidentiality, integrity, availability)$$

The highest value for the profile tags is used for each asset requirement—confidentiality, integrity, and availability. Next, a mapping in function "Q", is applied to transform the mean value into an integer as the final impact result, in the range of 1 to 100. The higher the impact, the more critical the asset in the organization.

Sample risk score calculation

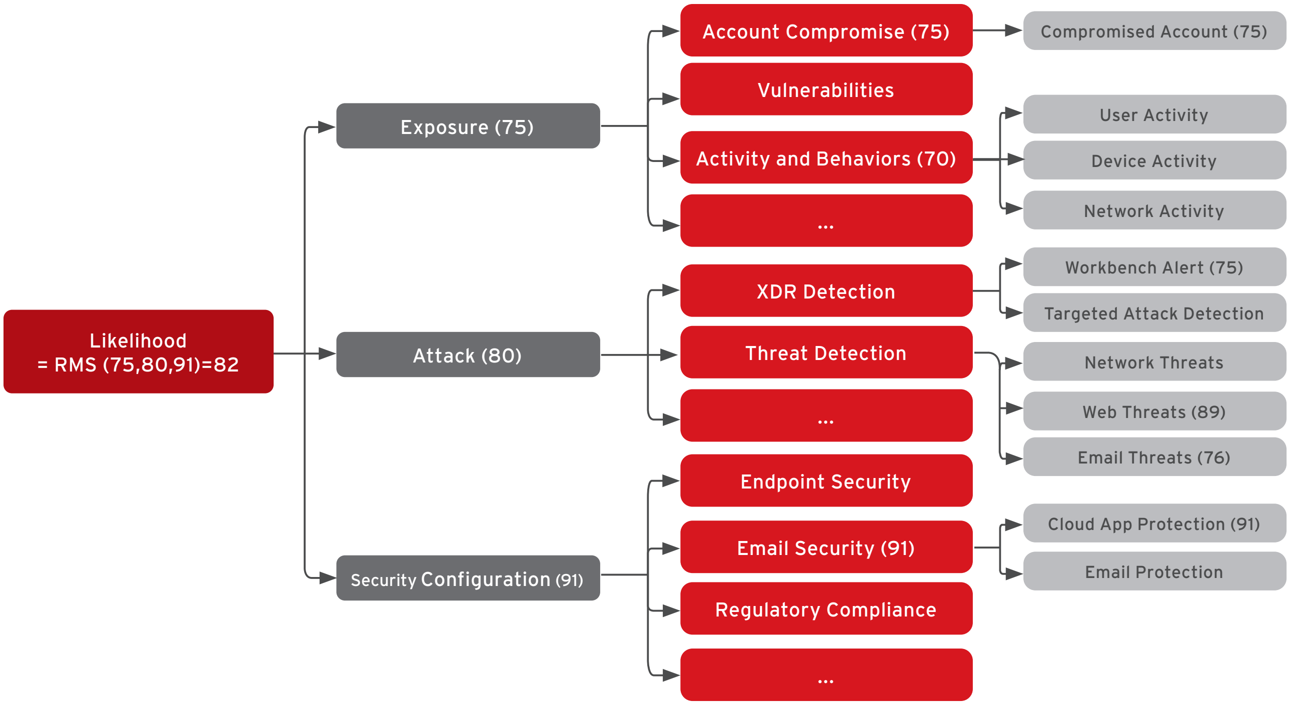
For example, consider a user asset with a risk score of 84. The risk score was calculated by assessing the likelihood score, which is calculated from the attack, exposure, and security configuration category events.

Following this example, suppose this user's account had a leaked account identification event scored 73, and an Microsoft Azure AD identity protection risk detection event scored 80. The weighted average of 75 rolls up into the compromised account indicator. (An indicator is a layer above the events. Other events also roll up their weighted averages into a relevant indicator.)

Then, the weighted averages from the indicator layer roll into a broader layer—factors—before eventually rolling up to the attack, exposure, and security configuration categories. Let's say the weighted averages for those three categories are 75, 80, and 91, respectively. We are then able to calculate the likelihood score for this asset.

$$likelihood = P(75,\ 80,\ 91) = 82$$

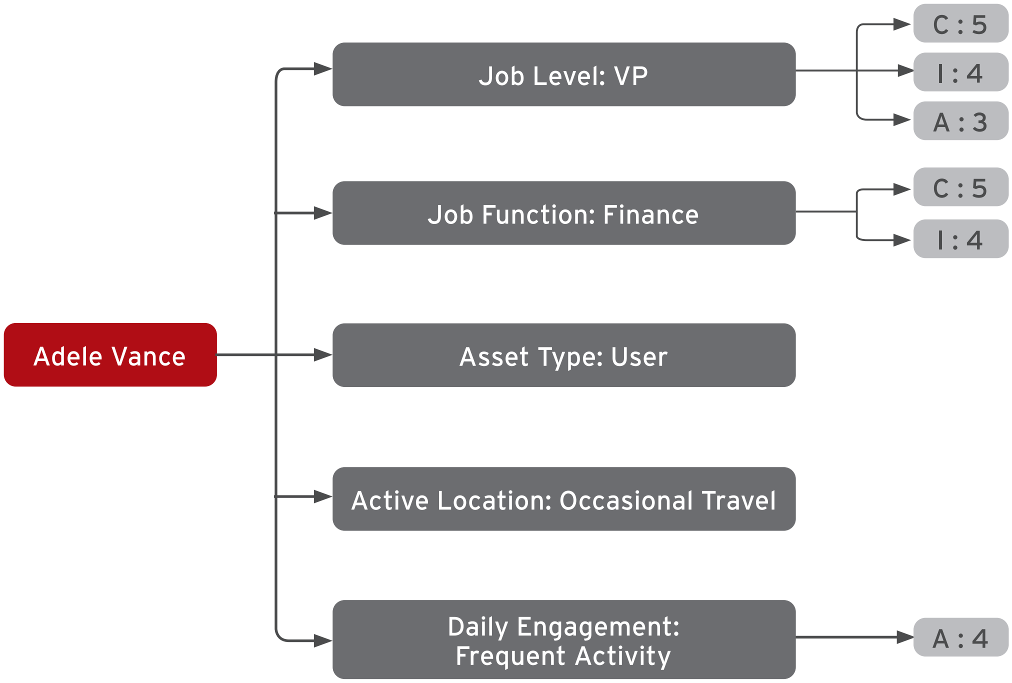
Figure 2: Example Likelihood Calculation



Impact is a calculation that uses the highest confidentiality, integrity, and availability requirements with a percentage mapping which transforms the impact value into the result of 87.

$$impact = Q(5, 4, 4) = 87$$

Figure 3: Deriving Impact from CIA Triad Requirements



Using the likelihood and impact, we can calculate the overall risk score for the user.

Therefore, this user's risk score is 84.

$$RiskScore = \sqrt{likelihood \cdot impact} = \sqrt{82 \cdot 87} = 84$$

This is a simplified version of the complex calculations continuously performed for all assets as new events are detected.

Risk index

Representing the overall risk to the organization in a mathematically fair manner, this index is calculated using the risk scores of a sampled set of assets. This sample includes all assets with risk scores in the High (70-100) range, a smaller sample of Medium-Risk (31-69) assets, and still a smaller sample of Low-Risk (1-30) assets. The actual amount of Medium-Risk and Low-Risk assets are determined using the average number of assets daily whose risk scores were rated as High within the last 30 days. This helps achieve a more comprehensive view of the risk to the organization.

The risk index is computed as the root mean square of all the high risk scores, the sampled medium risk scores, and the sampled low risk scores.

$$riskIndex \\ = \sqrt{(allHighRiskScores^2 + sampledMediumRiskScores^2 + sampledLowRiskScores^2)/3}$$

The exposure, attack, and security control indices provide the next layer of depth towards remediating and preventing risk in your organization. These issues provide additional visibility into your organization's security strategies, enabling the establishment of security strategies that reduce risk across the organization.

Attack index

This continuously monitored and updated figure indicates the maximum attack intensity of all cyber threats detected in the last 24 hours. An increase in the attack index is a substantial indicator that you may need to review and reinforce your security configuration. The attack index is calculated based on the number of known detections, impacted assets, and the severity of each unique threat type.

Trend Micro Vision One collects XDR telemetry from endpoints, email, networks, and the cloud to enrich threat detection for quicker remediation. It uses correlated threat data across these layers as hints toward identifying attacker activity and proposing multiple response actions. Overall, XDR enhances the accuracy of the attack index.

The attack intensity is computed approximately (as represented below by the wavy equals sign) as the total threat count over the number of impacted assets, multiplied by the impact as determined by the MITRE ATT&CK™ framework.

$$attackIntensity \approx \frac{totalThreatCount}{impactedAssetCount} \times impact$$

The attack index is the maximum $attackIntensity$ among all cyber threats in the last 24 hours.

$$attackIndex_{today} = max(attackIntensity_1, \dots, attackIntensity_n)$$

The attack index is continuously updated as new attack events emerge.

Exposure index

This reveals the risk of exposure to the organization through numerous factors, including the number and severity of unpatched vulnerabilities, misconfiguration of software, and the likelihood of exploitation impact. It is calculated using a sampled selection of assets' exposure events and their impacts over a 30-day period.

Given these formulas and the sampled assets (all the High-Risk exposure events and a subset of Medium-Risk exposure events and Low-Risk exposure events), we calculate the exposure index as the root mean square of the geometric mean of the weighted sum of exposure events and their impact.

$$\begin{gathered} exposureIndex = G(sampledAssets, exposureWeightedSum, impact) \\ exposureWeightedSum = P(exposure) \\ impact = M(attackSurface) \end{gathered}$$

Security configuration index

The security configuration index examines the status of an organization's security controls across different layers, products, and features. It lets analysts view and track system configuration trends over time. It is calculated using a sampled selection of assets' security configuration events over a 30-day period.

Similar to the exposure index, we calculate the security configuration index as the root mean square of the geometric mean of the weighted sum of security configuration events and their impact.

$$\begin{gathered} securityConfigurationIndex \\ = G(sampledAssets, securityConfigurationWeightedSum, impact) \\ securityConfigurationWeightedSum = P(securityConfiguration) \\ impact = M(attackSurface) \end{gathered}$$

Risk overview

The risk overview provides an at-a-glance understanding of your organization's security posture with a company-wide risk index, complemented by simplified Low, Medium, and High rankings for the exposure, attack, and security configuration indices.

As an example, assume that your exposure index is Low but your attack index is High. This clearly indicates that there is some attacking pressure on the organization but that you are well-configured and protected because your exposure is low. The risk overview is where to go when you wish to view high-level details regarding your organization's security posture.

The high-level nature of the risk overview illustrates a general idea of the overall risk to the organization—and which components are most vulnerable. From a single page, you gain insight into the overall risk score as determined by the likelihood and impact, the top risk factors and scores, trending, and peer comparison.

The risk overview also includes a prioritized list of at-risk assets based on the highest risk and measuring and weighing risk factors. The continuous and automated risk analysis provides deep insight into your organization. This takes a huge cognitive burden off of the security analysts and effectively communicates to the leadership teams so that prompt actions can be taken to respond to the threats.

Dynamic risk evaluation is the first critical step to minimizing digital exposure

Trend Micro Vision One provides custom, intelligent guidance, and recommendations to inform decision-making, enable accurate assessments, and prioritize risk remediation actions. Understanding the factors and formulas that make up the risk score arms you with the knowledge to reduce your risk score and improve your overall security posture.

Conclusion

Security teams can start by leveraging the company-wide risk index to make a high-level assessment of the organization's risk—the likelihood of a threat's occurrence and the potential impacts. The risk index considers the attack, exposure, and security configuration events that dive deeper into different high-level categories that make up risk.

With a comprehensive visualization of risk within your organization, you're able to anticipate and proactively secure your environment, detect and defend against threats and mitigate the impact of existing threats. Then, you can refine this process and develop a zero-trust architecture that is resilient in the face of even the most sophisticated attacks.

Risk insights can serve as the backbone of your organization's zero-trust journey with the continuous and in-depth monitoring demanded by the requirements of an effective zero-trust architecture. Closing the gaps identified by Trend Micro Vision One will correct your security posture over time and influence your actions to adhere to the zero-trust model. Furthermore, you join strength against the increasing amount and sophistication of threat actors by contributing to and using the vast intelligence gathered from other organizations that also rely on Trend Micro Vision One Risk Insights to establish an environment that is universally more secure against all manners of risk.

Risk evaluation scenario

Perhaps your exposure index stands out as high. So, you narrow in on it to explore which factors have recently affected it. From there, you may notice many vulnerabilities associated with a specific set of servers that have missed a recent critical update. Very quickly you've identified the greatest source of exposure to your organization with a clear indication of what became vulnerable and when.

The landscape of security defense and attacks are constantly evolving, and no organization can eliminate cybersecurity risk. However, continuous in-depth analysis of the organization's infrastructure and security risk posture will outline a clear path to defend and prevent future attacks of a similar nature. Following this response pattern will lower your risk score over time.