Technical Report

More than a Number: Your Risk Score Explained

Understanding risk score calculations

January, 2024
Trend Micro

Executive summary

Developing a resilient security posture requires a thorough and holistic understanding of the amount of risk faced by the systems and applications used in your corporate environment. Trend Vision One™ – Attack Surface Risk Management (ASRM) enables quicker, more accurate risk assessments through the surfacing of continuously updated metrics. This distills complex information into easy-to-understand individual asset risk scores in addition to a company-wide risk index.

Our Trend Vision One™ platform constantly monitors your 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
2. The potential impact of such an event

Using these factors, the platform presents the result as an integer between zero ("0") and 100, representing the overall risk to your organization's assets. With dynamic and accurate visibility into your current security posture, you can make informed decisions about prioritizing and addressing risk. Furthermore, your security analysts can perform manual or automated access control decisions based on your risk score and 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. This way, if an event occurs within the parameters of a security risk, the platform can remediate it by forcibly signing out or disabling the user entirely.

In the National Institute of Standards and Technology (NIST) ***Guide for Conducting Risk Assessments*** (NIST SP 800-30, Revision One), risk is defined as "a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." The publication also specifies that risks in this context include organizational assets, individuals, other organizations, the Nation, and organization operations including mission, functions, image, and even reputation.

Some organizations can tolerate a certain amount of risk. Quantifying it can help you decide whether to accept, mitigate, or avoid the risk entirely, enabling your security team to operationalize zero-trust architectures.

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 local area network (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 internet-of-things (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. Due to this ever-increasing complexity, a zero-trust security model requires continuous, in-depth monitoring. This ensures you have a complete picture of active and potential risks in your modern and dynamic environment.

Our Trend Micro™ Zero Trust Secure Access (ZTSA) solution is positioned to readily address these needs. 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 Vision One continuously recalculates risk scores to thwart attempted breaches at the earliest opportunity. Analysts can then use these scores to accurately determine which areas of your environment require attention, quickly assigning priority to the risks that must be addressed first.

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

The confidentiality, integrity, and availability (CIA) triad

The impact is the criticality of the asset as determined by business value. This value is based on the CIA triad outlined in NIST's ***Guide for Mapping Types of Information and Information Systems to Security Categories*** (NIST SP 800-60, Volume One, Revision One):

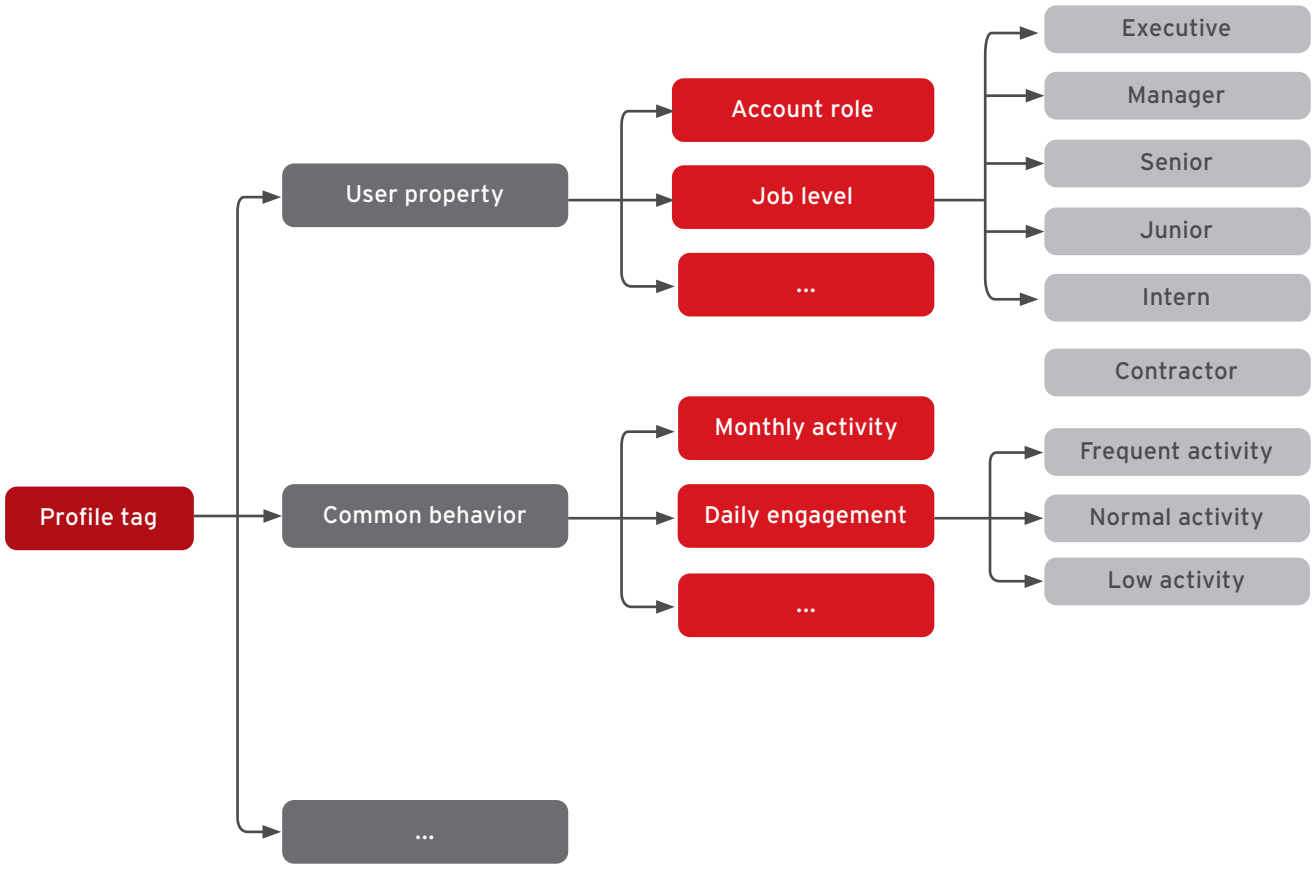
- **Confidentiality**: data, objects, and resources are protected from unauthorized access
- **Integrity**: data is protected from unauthorized changes to ensure reliability and correctness
- **Availability**: authorized users have access to the systems and resources they need

Trend Vision One monitors the attributes and behavior patterns that affect these three factors to assess their business value, representing them as profile tags.

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, user behaviors also have an impact. 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 confidential details that may affect future development and/or fundamental interests. If leaked, this data could cause catastrophic damage to your organization.
4	High	Contains highly sensitive details, the leakage of which could cause serious damage to your organization's security and interests.
3	Medium	Sensitive details that could damage the security and interests of your organization if leaked.
2	Low	Details that, while less sensitive, should only be disclosed internally. Otherwise, the dissemination of this information could cause minor damage to your organization's interests.
1	Very Low	Publicly available information, including public information-processing tools and system resources.

Integrity value definitions

Value	Level	Description
5	Very High	Unauthorized modifications or disruptions could have a significant, irreparable impact on your organization and business.
4	High	Unauthorized modifications or disruptions could have a significant impact on your organization, along with a potentially severe business impact. These will be more difficult to remediate.
3	Medium	Unauthorized modifications or disruptions could have a noticeable impact on your organization and, to a significant degree, its business. However, it may be possible to remediate said impact.
2	Low	Unauthorized modifications or disruptions could have a minor impact on your organization. Business impact will likely be minor and easily remediated.
1	Very Low	Unauthorized modifications or disruptions would have a negligible impact on your organization.

Availability value definitions

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

Calculating risk scores

Trend Vision One incorporates an array of factors into the risk score, including your configuration of security controls, asset criticality, vulnerabilities, and threat activity. The platform then formulates a risk score for each asset type and an index for your entire organization. The result is an integer between zero ("0") and 100 that falls into one of three levels, as shown on the right.

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

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

While the risk score calculation process is complex, it can be summarized as the geometric mean of the likelihood and the impact—in other words, by multiplying the likelihood by the impact and calculating the square root of the product, as follows:

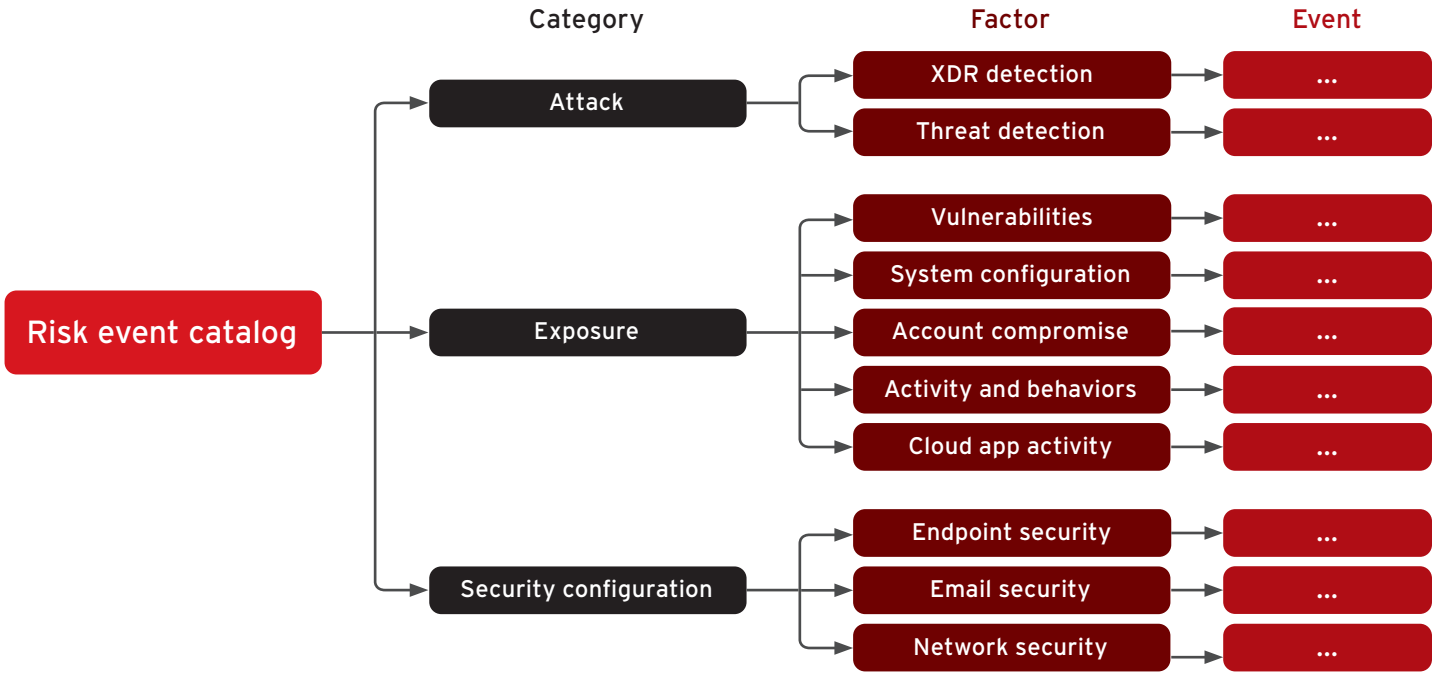
$$RiskScore = \sqrt{likelihood \times impact}$$

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

Risk events, factors, and categories

Risk assessments conducted through the Trend Vision One platform are based on more than 1,000 risk events. Each of these is a basic unit to be assessed for risk. All telemetry data, detections, XDR alerts, vulnerabilities, and other events from Trend and third-party solutions are collected, detected, and converted into these events, which are organized in a risk-oriented catalog along with three categories and 10 factors as illustrated below.

Figure 2: risk event catalog



The three applicable categories within this catalog function as follows:

Attack category

This helps to determine the likelihood of an attack by capturing threat detections from various security modules including the security analytics engine. In turn, this captures previous and existing threat activity as well as relevant data to help predict future malicious movement.

Exposure category

This represents weaknesses within your environment that could potentially be exploited. These include common vulnerabilities and exposures (CVEs), security and cloud misconfigurations, compromised accounts, and abnormal activity from users, devices, and cloud apps.

Security configuration category

This considers the deployed and missing security controls within your environment including endpoint protection solutions and specific feature sets like behavioral monitoring. If your organization is sufficiently configured, it is better protected and considered less likely to experience an attack.

The weighted sum calculations for these three categories are represented in the equation further below. The events in question are generated using telemetry from your organization's existing security stack. This includes any Trend solutions in use as well as application programming interface (API) integrations with security information and event management (SIEM), security orchestration, automation, and response (SOAR), identity access management (IAM), firewall, threat intelligence, IT service management, and ticketing solutions.

Likelihood

Risk events in Trend Vision One are assessed from a likelihood and impact perspective. Likelihood represents the probability that the event in question will occur or exploit a specific asset, while impact describes the magnitude of harm that would be inflicted on said asset.

The likelihood that a risk event could exploit a weakness in your IT infrastructure—either directly or through a chain of vulnerabilities—is converted into a weighted risk category based on probability. This is evaluated based on an individual asset's attack, exposure, and security configuration categories in the following equation:

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

Here, "P" is a function that considers the likelihood from all the detected events pertaining to the asset in question in these categories. Each category receives a score between one and 100. Higher scores indicate more severe security issues, and more recent events have a greater impact on the likelihood evaluation.

Impact

Defined as the magnitude of harm that a breach can be expected to cause your organization, the impact is effectively the attack surface as determined by evaluating asset criticality. This evaluation is based on the aforementioned CIA triad, serving as a summary of the requirements from all the business-related profile tags for the asset in question. The impact is calculated from these requirements, featuring a score between one and five, as per the following equation:

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

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, which has a range between one and 100. The higher the impact, the more critical the asset is within your organization, which is similar to calculating likelihood.

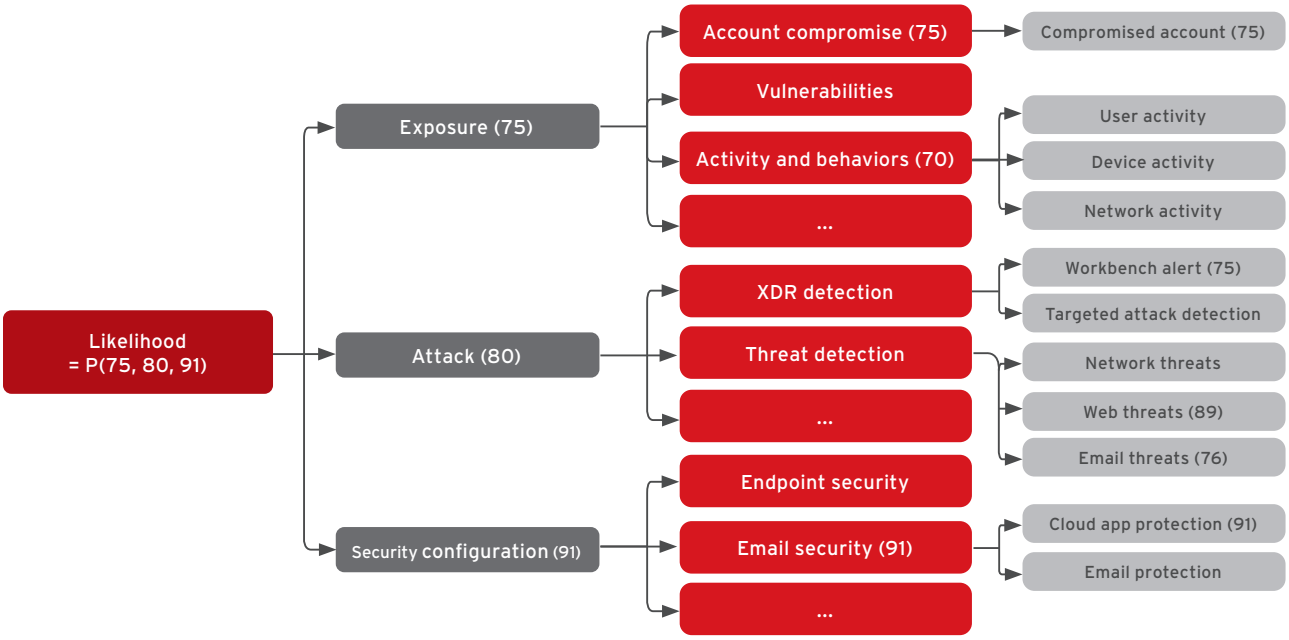
Sample risk score calculation

As an example, consider a user asset with a risk score of 84. The risk score was calculated by assessing the likelihood score, which itself is calculated from the attack, exposure, and security configuration category events. Let's say that a leaked account identification event scored 73 on this user's account, and a Microsoft Entra ID Protection risk detection event scored 80. A weighted average of 75 rolls up into the compromised account indicator, which is a layer situated 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 these three categories are 75, 80, and 91, respectively. We are then able to calculate the likelihood score for this asset, as demonstrated below:

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

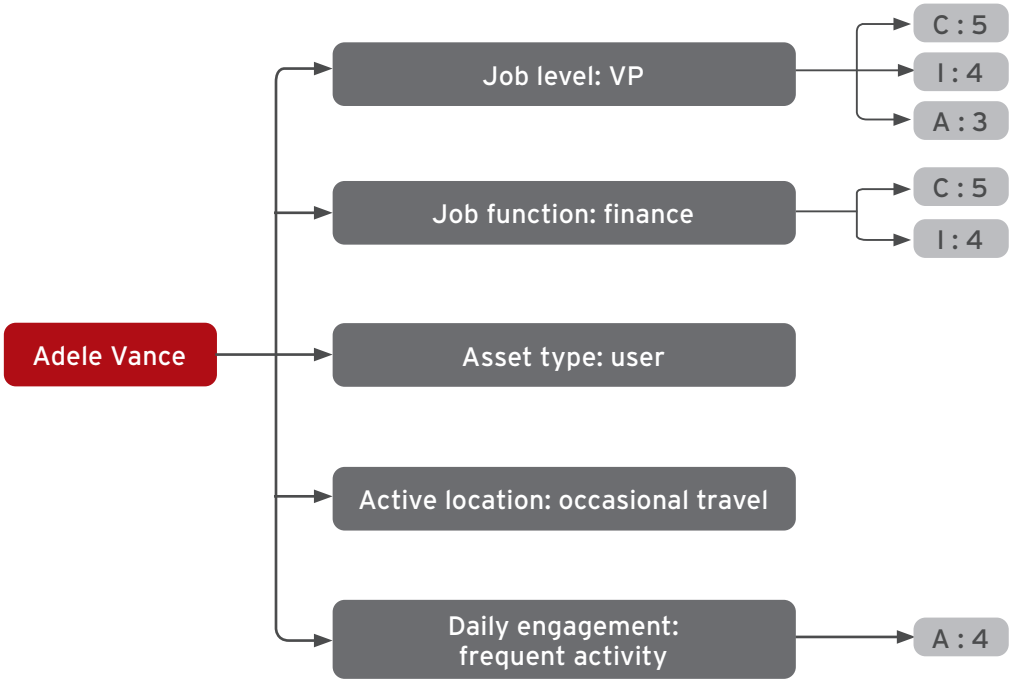
Figure 3: example likelihood calculation



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 as shown below:

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

Figure 4: deriving impact from CIA triad requirements



Now that we have calculated the likelihood and impact, we can determine the overall risk score for the user:

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

The result is a risk score is 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 your organization in a mathematically fair manner, this index is calculated in a weight summation method, using the risk scores from all the generated risk events. The calculation process obtains the factor scores directly from their subsidiary risk events. When these events occur, such as attacks in the lateral movement or impact phases, zero-day vulnerabilities, the factor scores are amplified and highlighted in the algorithm implemented in function "F," as shown below:

$$FactorScore = F(event\_score_1, \ldots, event\_score_n)$$

This results in identifying category scores by summarizing the weight of contributing factors, as detailed here:

$$CategoryScore = sum(Wf_1 * FactorScore_1, \ \ldots \ , Wf_n * FactorScore_n)$$

(Factors = XDR detection/Threat detection/Vulnerabilities/System configuration/Account compromise/Activity and behaviors/Cloud app activity/Endpoint security/Email security/Network security)

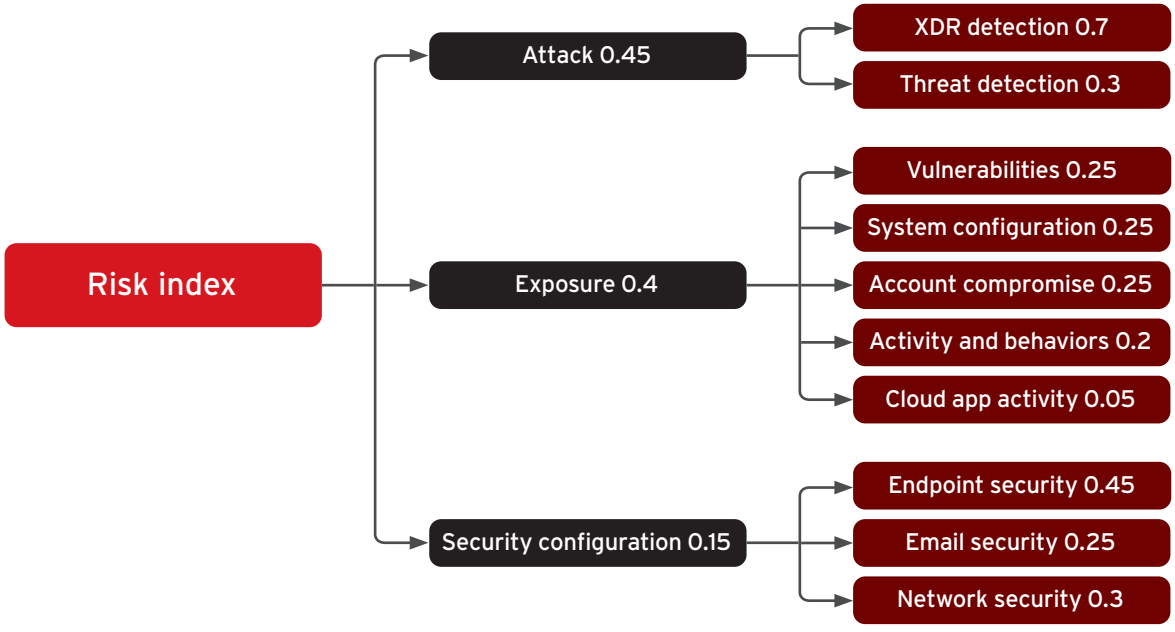
Lastly, there is the risk index, a weight summary of the three categories in question, as shown below:

$$RiskIndex = sum(Wc_1 * CategoryScore_1, Wc_2 * CategoryScore_2, Wc_3 * CategoryScore_3)$$

(Categories = Attack/Exposure/Security configuration)

Weights for category scores and risk indexes are pre-defined by security experts, as shown in figure five below. These weights may be adjusted for irregular or long-term formats, such as for product research and development. Once they are applied to your environment, a weight "calibration" process needs to be completed, which will reveal the status of your risk assessment visibility and capability. This process utilizes customer-enabled data sources derived from our ASRM solution. Through a combination of pre-defined weights and customer-enabled data sources, information is generated and applied based on relevant, real-world scenarios.

Figure 5: initial weight settings for risk index calculation



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 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 to identify attacker activity while proposing multiple response actions. Overall, XDR enhances the accuracy of the attack index.

The attack intensity is computed approximately—as represented by the two stacked tildes in the equation below (≈)—as the total threat count over the number of impacted assets. This is then multiplied by the impact 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, as demonstrated below. This is continuously updated as new attack events emerge.

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

Exposure index

This index reveals the risk of exposure to your organization through numerous factors. These include the number and severity of unpatched vulnerabilities, software misconfigurations, and the likelihood of exploitation impact.

The exposure index is calculated using the same pre-defined and calibrated weights used for risk index calculation. In this case, however, only those related to exposure-category events are factored into the equation. When risk events for time-critical vulnerabilities happen, such as zero-day exploits, the factor score would be amplified and highlighted in the algorithm implemented in function "G." The full equation is detailed below. Once this is complete, we obtain the exposure category scores by summarizing the weight of contributing factors:

$$FactorScore = G(event\_score_1, \ldots, event\_score_n)$$

$$ExposureIndex = ExposureScore = sum(Wf_1 * FactorScore_1, \ \ldots\ , Wf_n * FactorScore_n)$$

(Factors = Vulnerabilities/System configuration/Account compromise/Activity and behaviors/Cloud app activity)

Security configuration index

The security configuration index examines the status of your organization's security controls across different layers, solutions, and features. It allows analysts to view and track system configuration trends over time. This index is calculated using the same pre-defined and calibrated weights as used in the risk index calculation, but only those related to events in the security configuration category, as demonstrated below:

$$FactorScore = H(event\_score_1, \ldots, event\_score_n)$$

Next, we obtain the security configuration category score by summarizing the weight of contributing factors, as demonstrated here:

$$SecurityConfigurationIndex = SecurityConfigurationScore$$
$$= sum(Wf_1 * FactorScore_1, \ \ldots\ , Wf_n * FactorScore_n)$$

(Factors = Endpoint security/Email security/Network security)

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 exposure, attack, and security configuration catalogs.

As an example, let's say that your exposure index is low, but your attack index is high. This indicates that there is some attacking pressure on the organization, but you are well-configured and protected because your exposure is low. This 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—including 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, trends, and peer comparisons.

The risk overview also includes a prioritized list of at-risk assets, which is based on the highest risk along with the measurement and weight of its contributing factors. Continuous and automated risk analysis provides deep insight into your organization. This takes a huge cognitive burden off your security analysts while effectively communicating appropriate and prompt threat response actions to leadership teams.

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

Trend 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 contributing towards your risk score arms you with the knowledge needed to reduce it and improve your overall security posture.

Harness visualization and insights to enhance your operational security

Security teams have the capability to leverage your company-wide risk indexes to make a high-level assessment of threat occurrences and potential impacts. As we've explored, this process considers the attack, exposure, and security configuration events affecting your operations.

With a comprehensive visualization of risk within your organization comes the enhanced ability to anticipate risk elements and proactively secure your environment, detect and defend against threats, and mitigate their impact. 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 while meeting the understandably strict continuous in-depth monitoring requirements that such an architecture demands. Closing the gaps identified by Trend Vision One will correct your security posture over time, better enabling your actions to adhere to the zero-trust model. In addition, you'll be joining the fight against an ever-increasing number of sophisticated threat actors by contributing to—and using—the vast intelligence gathered from other organizations harnessing ZTSA to establish a universally more secure environment.