Getting Started with Trend Vision One: Attack Surface Risk Management (ASRM)

Student Guide

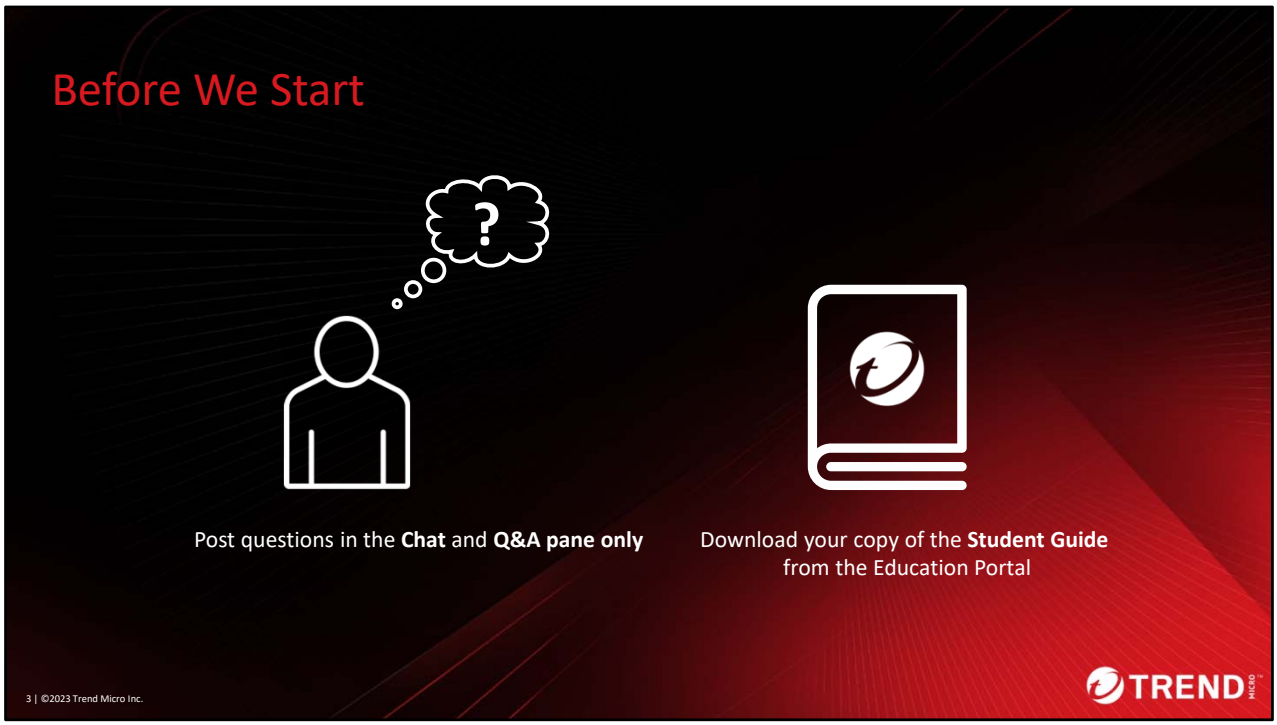
May, 2024

TrendMicro.com

We are excited to introduce you to Trend's cornerstone exposure management solution that is part of the Trend Vision One platform.

This session is designed to assist IT managers, operations teams, CISOs, and CIOs in adopting a risk-based cybersecurity approach to address evolving challenges in the cybersecurity landscape.

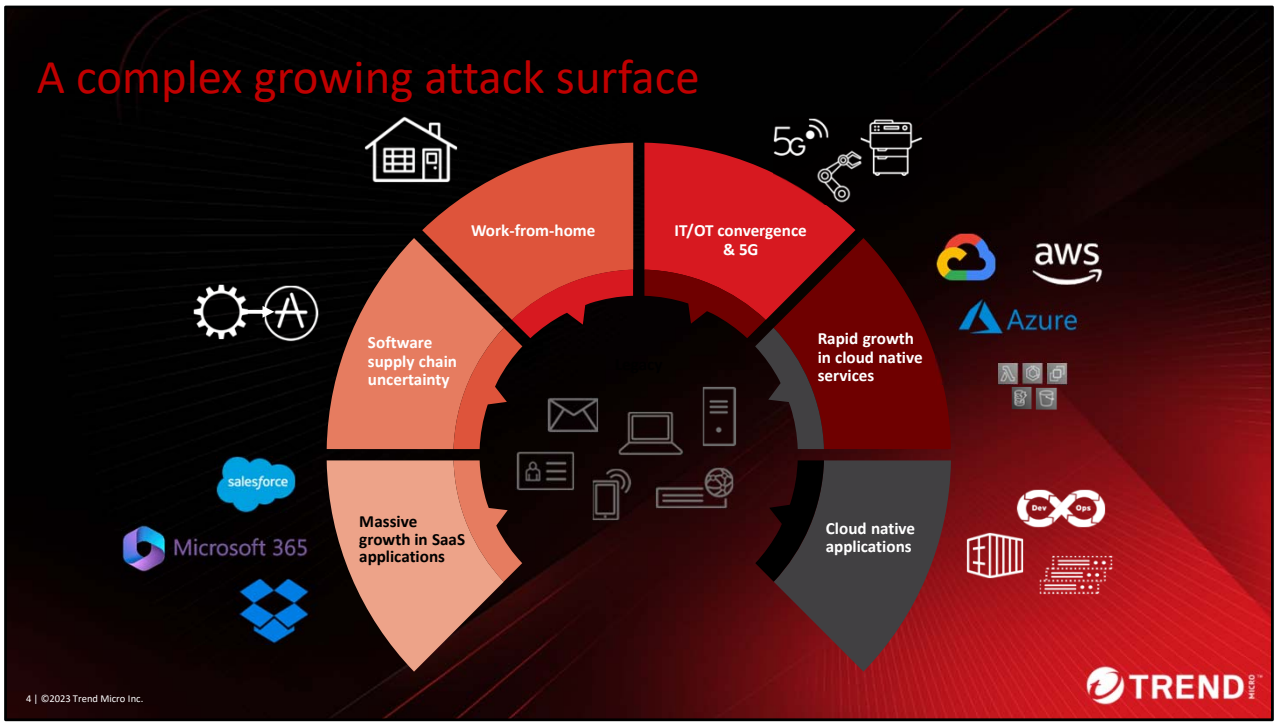
We will explore how Vision One Attack Surface Risk Management (ASRM) helps calculate your cybersecurity risk and explains it to various stakeholders, from the board to those who need to act based on this risk. Additionally, we'll delve into using the Executive and Operations dashboards, along with Attack Surface Discovery, to understand and mitigate risk. Most importantly, we'll examine the necessary steps to lower your organization's risk using the provided risk management tools. Finally, we'll explore integrating third-party products into Vision One and maximizing data sources, enhancing Vision One's discovery capabilities for a more comprehensive and accurate view of your organization's security posture.



Post any questions in the **Q&A** pane. The **Chat** pane is not being monitored by the trainers.

The Student Guide for this course can be downloaded from the Trend Education Portal.

- Log into your account, click the **Getting Started With Attack Surface Risk Management** course.
- Scroll to the **Course Syllabus** section and click to download the Student Guide PDF.

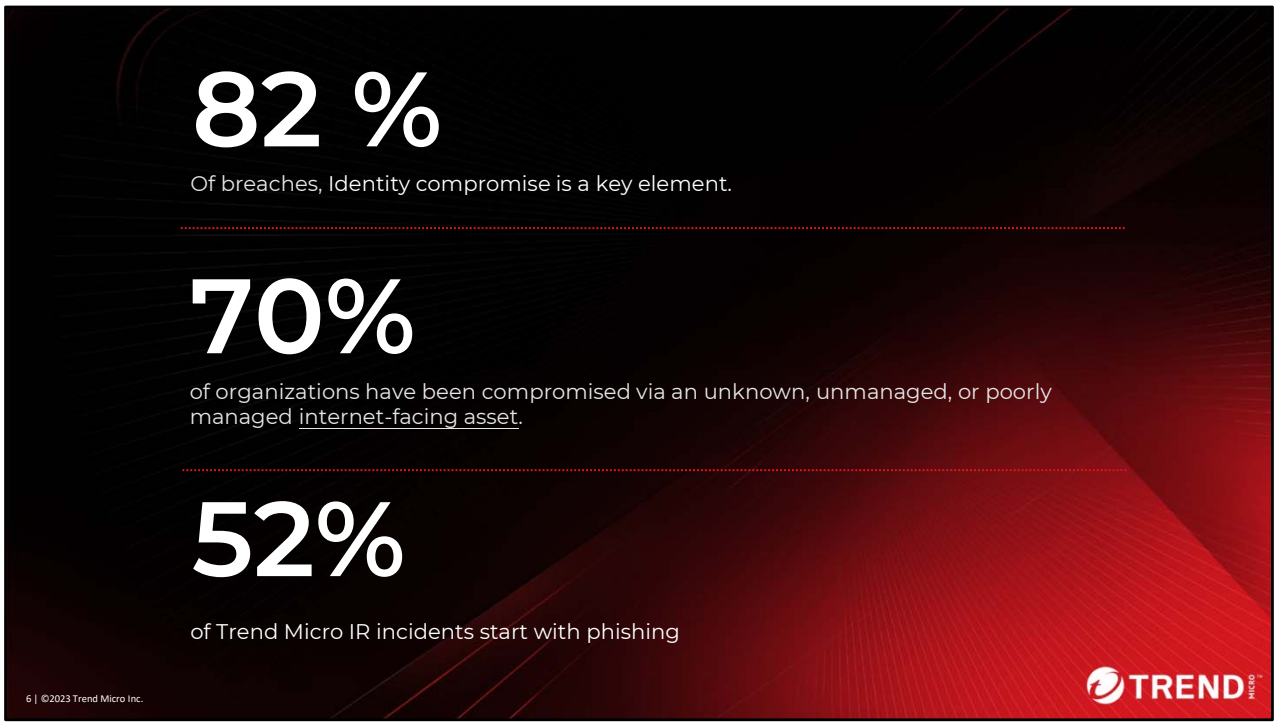


The threat landscape is always changing, but the drastic shifts of recent years have made unprecedented demands of security teams.

- Attackers are trying to attack in all kinds of new ways and new places.
- The battleground never stops growing and changing.
- This very complex and diverse digital environment presents new opportunities for attack.
- An increased number of cyber assets means more of those assets are likely to be vulnerable, more areas of weakness arise in the infrastructure, and, overall, results in an even bigger and more profitable target that cybercriminals are only too eager to exploit.

The attack surface refers to all cyber assets and all the attack vectors you are facing. When it comes to your attack surface, you can no longer consider only assets like endpoints, servers and workloads, but now must consider identities, mobile devices, IoT, OT, cloud infrastructure and so on.

- Facing the perfect storm: Ever-growing number of cyber assets in your organization on one side, and on the other, attackers who continue to find new and novel ways of infiltrating organizations and systems. You need to understand the attack surface. Asking and answering things like:
  - Which assets present an easier challenge for attackers?
  - How impactful would it be if that specific asset is compromised?
  - Does it host sensitive data, or belong to VIP employee in your company, like an executive?
  - What is its relationship or connection with other assets?
- Depending on skills, resources, and available tools in your organization, the difficulty in getting to these answers could range from tedious to impossible.



Due to this attack surface scale in the past year alone, nearly 70% of organizations have been compromised via an unknown, unmanaged, or poorly managed internet-facing asset.

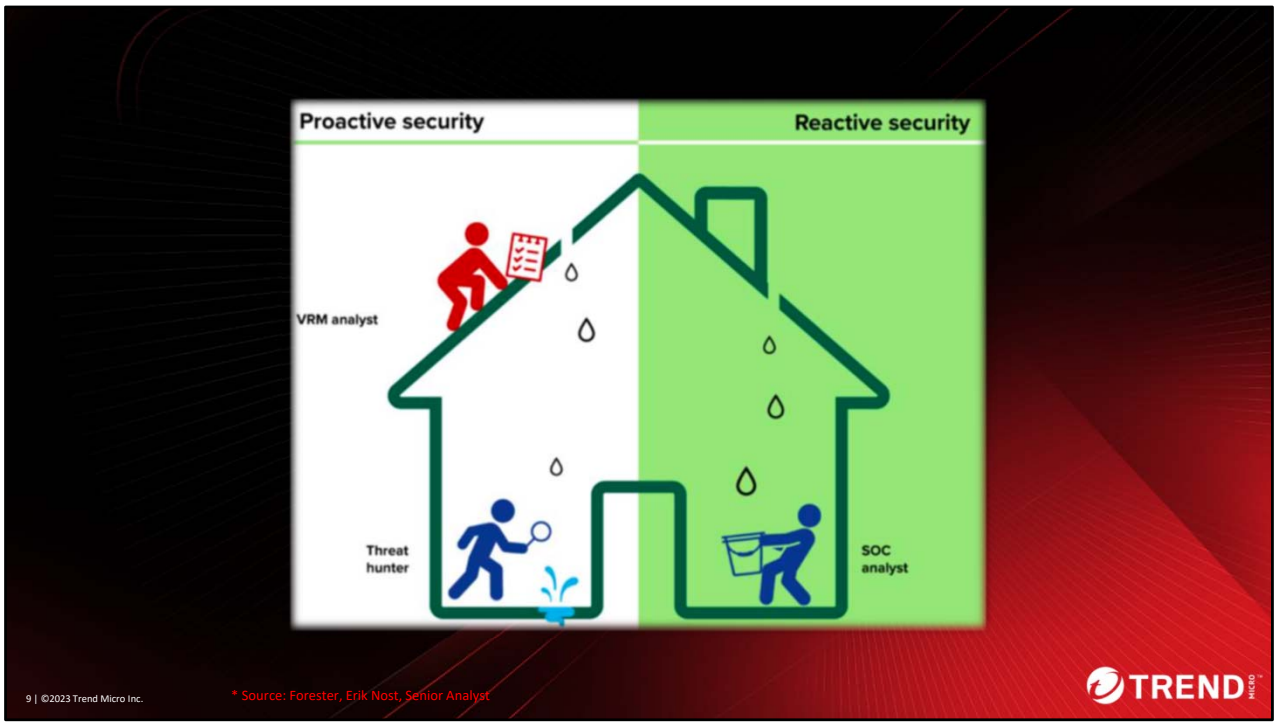
This is partly due to the complexity of taking an inventory of external-facing assets — with the average organization taking upwards of 80 hours to generate an accurate picture of their attack surface.

Source: https://www.randori.com/reports/the-state-of-attack-surface-management-2022/

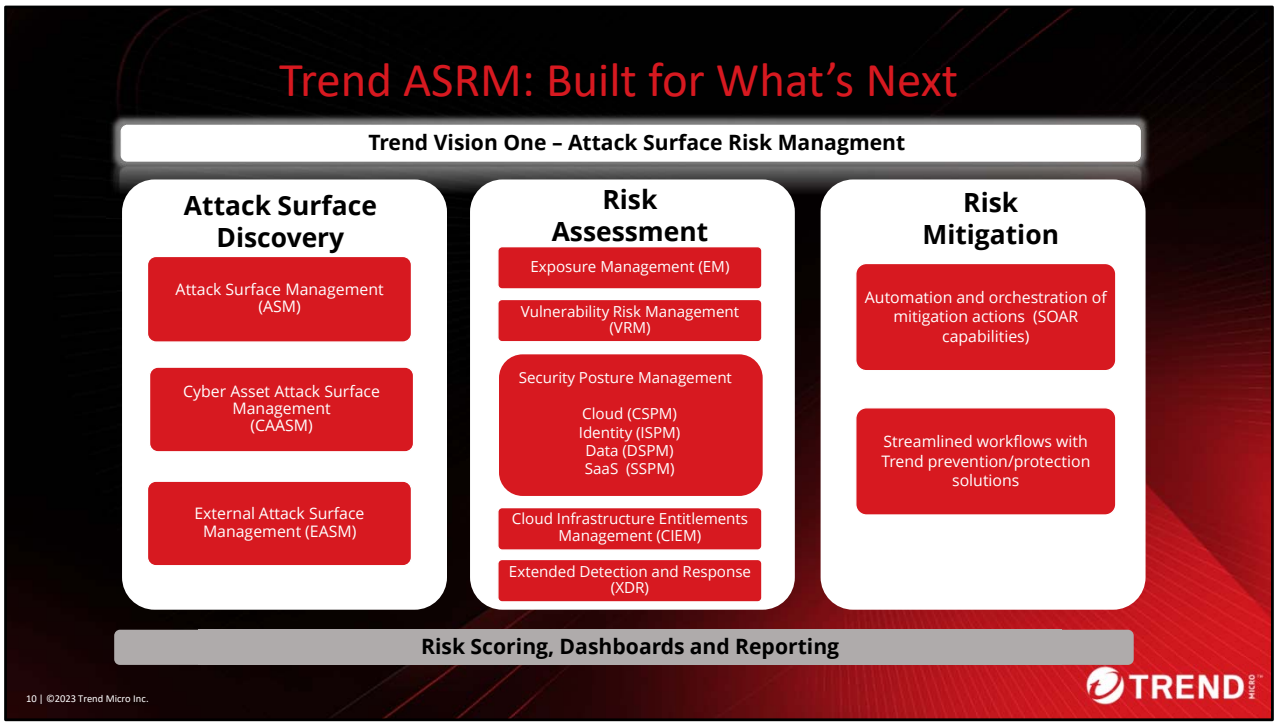
You are probably already familiar with Trend's ASRM Lifecycle (Discover, Assess, Mitigate).

With Attack Surface Risk Management capabilities in Vision One, we offer customers a full cyber risk lifecycle management solution helping you become more **proactive** at identifying potential risk, and mitigating or remediating it before that risk can be realized in the form of a breach or incident.

To manage risk effectively - now more than ever organizations need full holistic visibility. This is essential for addressing critical questions that risk decision-makers grapple with, ultimately improving their overall management of risk exposure.



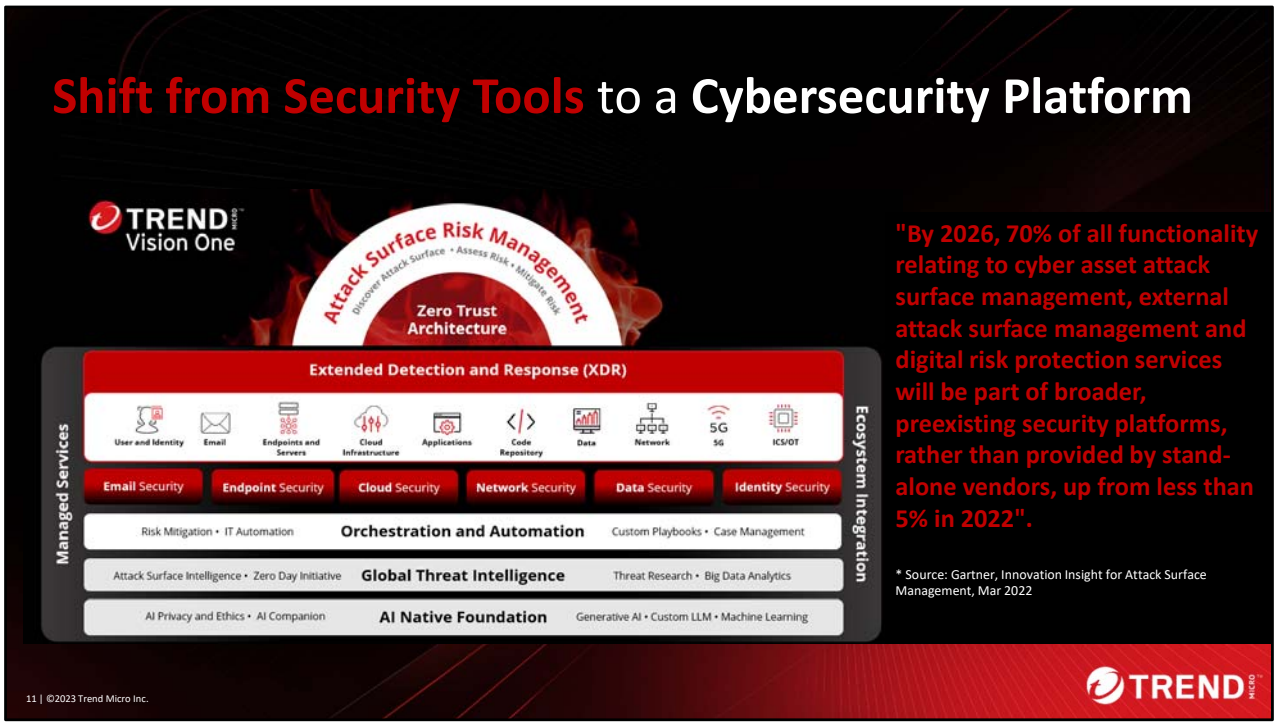
This illustration (Erik Nost, Senior Analyst at Forester) simplifies the concepts of “proactive” versus “reactive” security approaches using a house analogy to illustrate fixing a leak. When it comes to ASRM (proactive security), it’s about staying ahead of the game and safeguarding your organization’s digital landscape.



Trend's ASRM is built to manage the full cyber risk lifecycle and it collapses multiple market capabilities into one offering. It has the broadest and deepest capability set on the market. Why get one thing when you can get everything you need to manage risk and ease the burden on your team with prioritization and central management built-in.

Unlike other Attack Surface Management (ASM) vendors it goes beyond discovery with **assessment** and **remediation**.

- From point products by assessing risk across the attack surface, as opposed to looking at risk in individual areas or for specific vectors.
- From other Risk Scoring/ Dashboard solutions by being able to assess a broader set of risk factors.
- From a risk assessment perspective in particular, no other vendor offers the option to consider or calculate risk across so many factors. We offer risk scoring across cloud assets, internet-facing assets, devices, cloud app activity, account compromise, user activity and behaviors, vulnerabilities, XDR detections, and threats. This offers a comprehensive assessment of risk, as compared to competitor's siloed risk views or "checkbox" capabilities without any integrations between all of the risk factors.
- From key competitors by offering a platform approach that consolidates XDR and helps operationalize Zero Trust strategies.



More and more customers are moving towards a consolidated platform approach and Trend Vision One is uniquely positioned to help you move in that direction at your own pace.

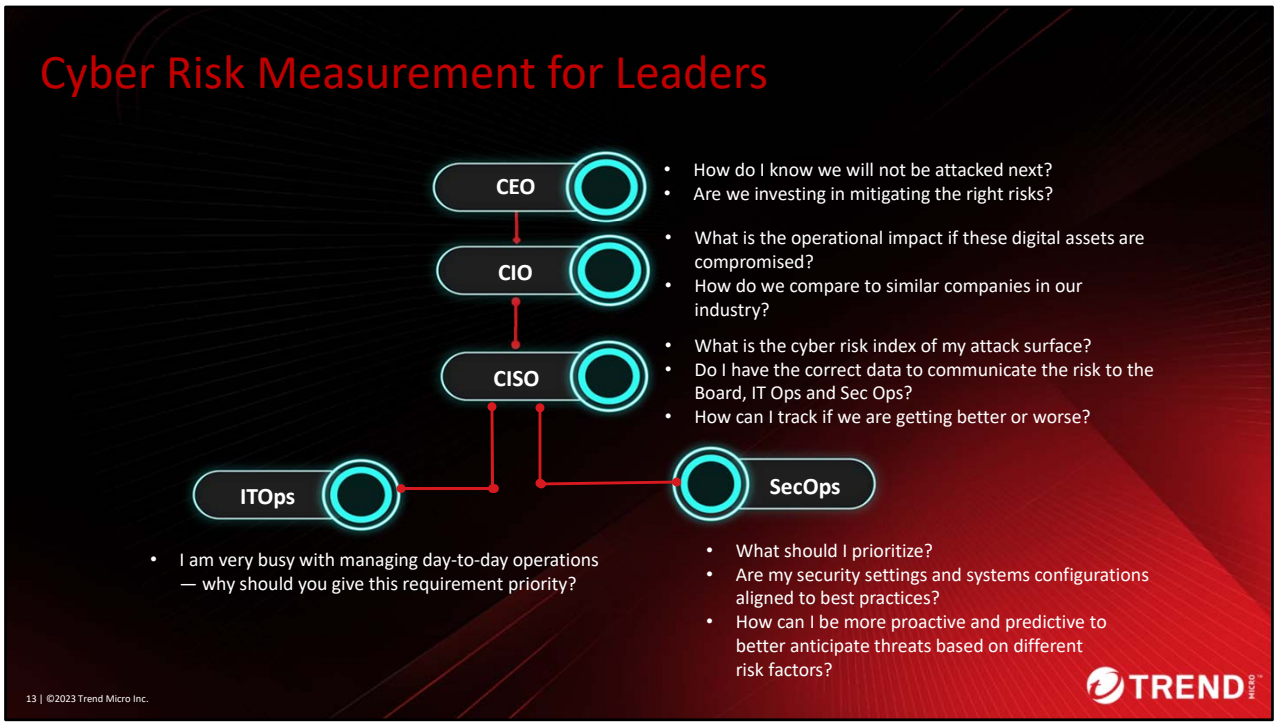
The Trend Vision One platform represents a truly integrated approach and visibility across the entire digital environment.

- The platform includes the solutions, services, and technology that connect and benefit security and operations teams across multiple functions.
- More importantly, the platform delivers a single common framework so security teams can bridge threat protection and cyber risk management to drive better security outcomes and accelerate the business.

During today's session, we will delve into the significant role that comprehensive risk management plays in ASRM.

ASRM today is helping our customers answer some extremely important questions, questions that you might be asking yourself like:

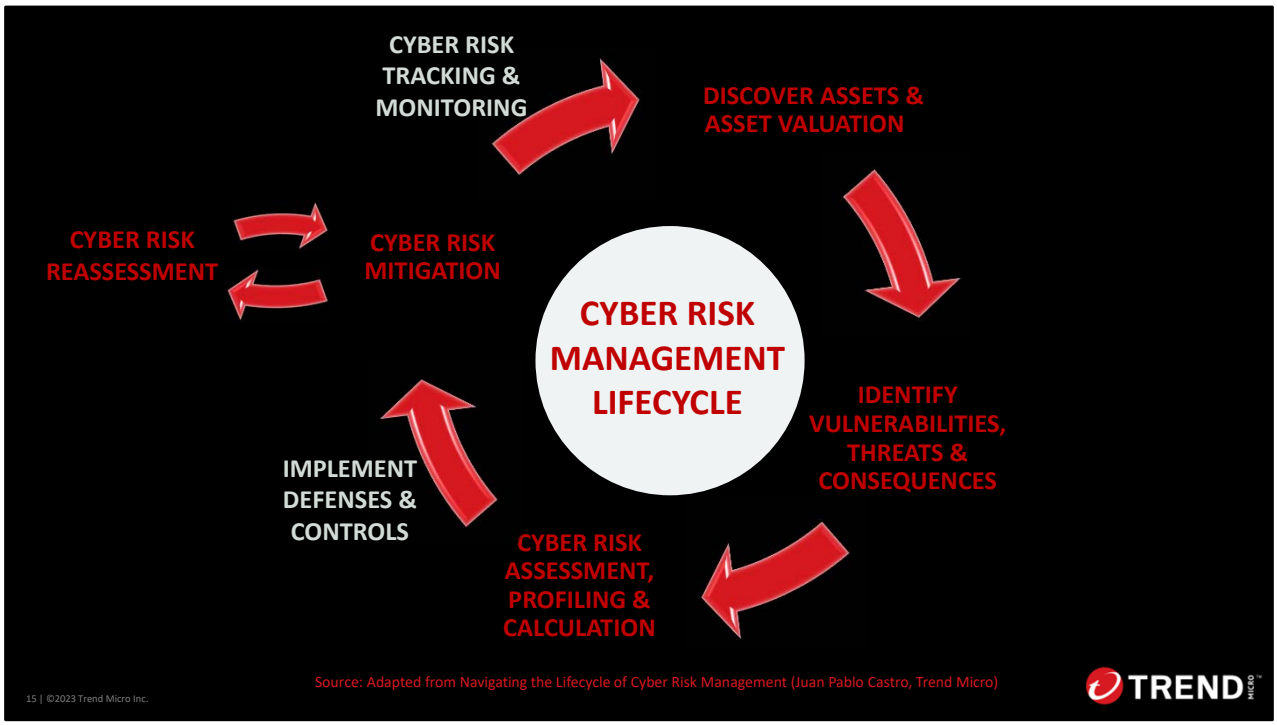
- **Why is my Risk Index 57?** (or whatever that number may be) Understanding risk calculation is crucial for risk management, stakeholder communication, and risk reduction. Considering factors like threats, vulnerabilities, and potential consequences, understanding your risk assessment helps identify risks and their relative importance.
- **Do I have complete visibility of risks in my environment?** One of the most pressing concerns today is about risk visibility and if you have complete visibility of your environment.
- **Are we compliant?** If not, how do we get and stay there? Another critical area of concern is compliance. Its not just about being compliant in a point of time but getting compliance and then staying compliant.
- **How do I make the best use of my team, technology and time?** Customers are asking if we can address their need to reduce complexity and cost. How can they make the best use of their team (big or small) their existing investments and the time.
- **What steps should/could I take to lessen chances of an attack?** Improving cyber resilience is top of mind and what steps should/could they be taking to ensure they are as secure as can be. I am sure one or all these questions are on your mind as well.



Understanding the questions that security personas need answers to is crucial for effective risk management. Let's explore some common inquiries that security professionals encounter.

Addressing these questions helps organizations **quantify** cyber risks and make informed decisions. By understanding the risks thoroughly, security leaders can communicate effectively both upstream and downstream, helping you maintain a healthy security posture.

But before diving into risk discussions with stakeholders and adopting a risk-based approach to cybersecurity, it’s essential to first understand the fundamentals of the Cyber Risk Management Lifecycle.



The following cyber risk management lifecycle, adapted from Juan Pablo Castro at Trend Micro, serves as a strategic compass for navigating the complexities of digital threats. While numerous sources, such as this one (https://medium.com/@jp_castro/navigating-the-lifecycle-of-cyber-risk-management-a-strategic-blueprint-d810abdc5b69) offer further insights, we will provide a concise overview here.

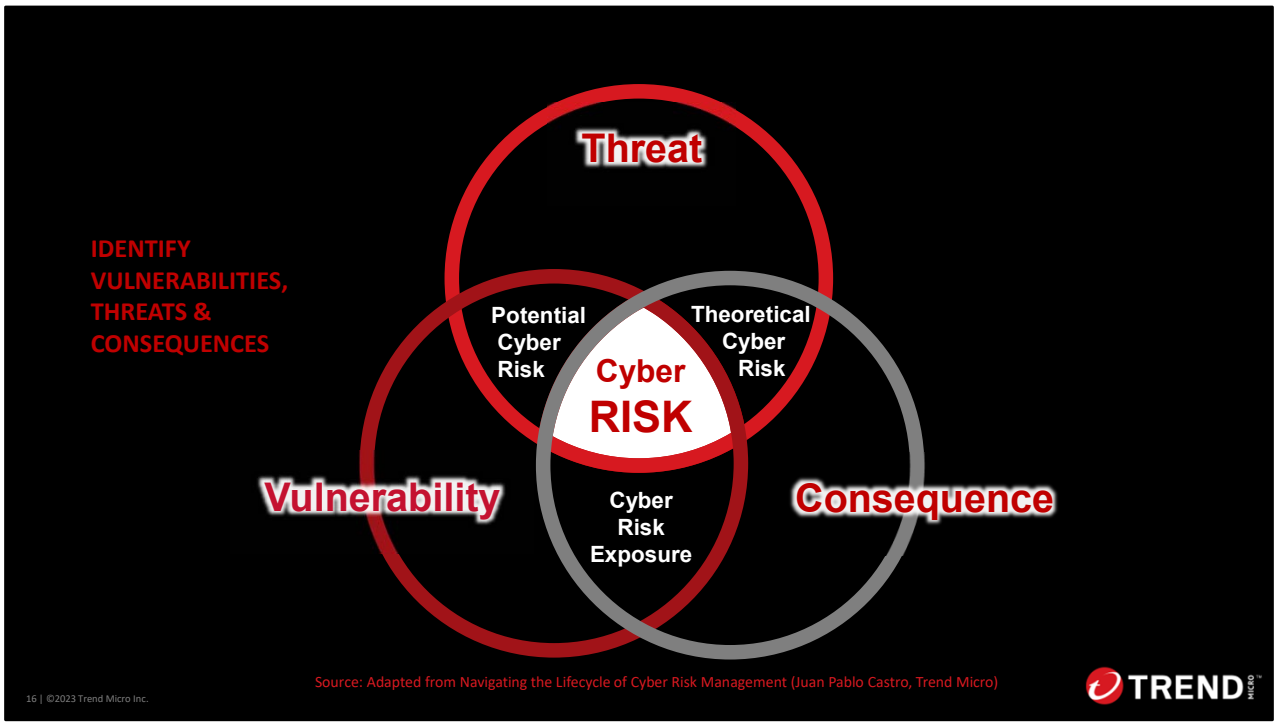
This lifecycle is not just a framework; it's a structured methodology guiding organizations through the complex terrain of digital threats.
The Cyber Risk Management Lifecycle facilitates this by providing a structured methodology to identify, assess, mitigate, and monitor cyber risks in a continuous loop of improvement.

It empowers businesses to swiftly adapt to the dynamic landscape of cyber threats, fostering agility and informed decision-making. This strategy guarantees that cybersecurity initiatives are not merely reactive responses but are seamlessly integrated into the organizational strategy. By implementing proactive defense mechanisms, it safeguards vital assets while facilitating business growth and innovation.

1. The lifecycle begins with discovering every asset and assigning a valuation to each one. It's crucial to set the context and criticality of every asset, as this forms the foundation for managing cyber risk. Without this, it is not possible to manage cybersecurity risk. This process involves identifying all assets and how they are related, including IPs, PCs,

desktops, containers, Lambda functions, APIs, websites, and more. This process is very complex.
    - While companies can utilize a variety of tools within their technology stack to manage assets, the real challenge lies in maintaining an updated asset list and comprehending the criticality of each asset. Platforms like Vision One automates this process, allowing you to update asset criticality starting with a solid baseline.
    - This initial phase of discovering assets and assessing their criticality is key to the Cyber Risk Management Lifecycle.
1. The second phase involves identifying vulnerabilities, threats, and consequences associated with the discovered assets. This step is crucial as it forms the basis of the risk definition.
2. Once these elements are identified, the next step is to assess and calculate the cyber risk. This involves not only identifying these factors but also quantifying them in a measurable way, such as with risk scoring.
3. After assessing the risk, the next step is to implement defenses and controls to mitigate the cyber risk. This is a critical part of the Cyber Risk Management Lifecycle, unique to managing cyber risks. It's important to note that cyber risk management is part of operational or IT risk management, which are handled differently and require a different approach.
4. Following mitigation, continuous tracking and monitoring are essential. Unlike static methods like GRC (Governance, Risk, and Compliance), continuous monitoring ensures that risks are actively managed, not just assessed periodically.
5. After mitigation and monitoring, continuous reassessment and recalculation of cyber risk is necessary. This **continuous** cycle ensures that risks are managed dynamically, adapting to changes in the risk landscape.

Imagine for a moment having to perform all these steps using only your own tools and resources!



The definitions of threats, vulnerabilities, and consequences are crucial for understanding cyber risk.

- Threat refers to anything that has the potential to cause harm or allow unauthorized access to an information system. This could be malicious actors, state-sponsored groups, cyber criminals or insider threats.
- Vulnerability is a weakness that can be exploited by a threat. Examples include unpatched software, misconfigured controls and users who may fall victim to social engineering.
- Consequence is the impact or damage that would occur if a threat successfully exploits a vulnerability. Financial loss, reputational harm, loss of proprietary data, and business disruption are common consequences.

Understanding the relationships between threat, consequence, and vulnerability is key to comprehending and effectively managing cyber risk.
Visualizing them as intersecting circles helps illustrate their **relationship**. Remember that having all three components is necessary for a cyber risk to exist.
For example,

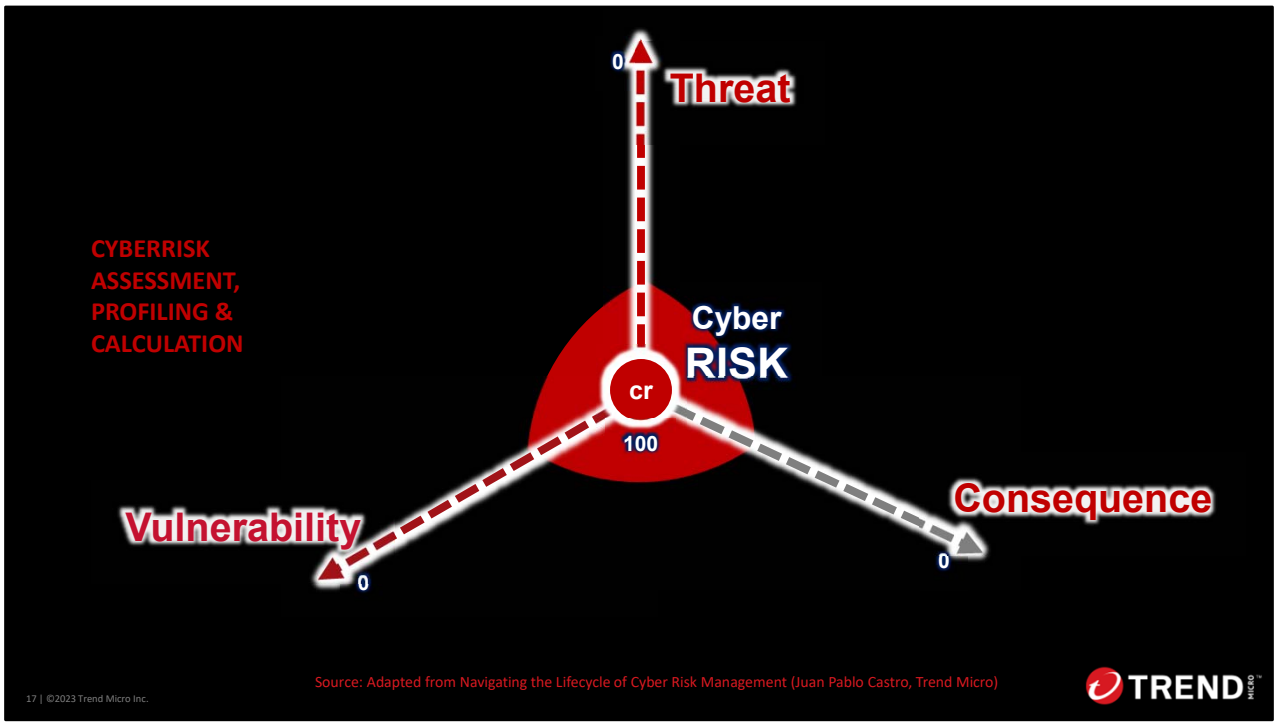
- If only threats and vulnerabilities are present, you do not have a cybersecurity risk, you have a **potential** risk.
- If you have threats and consequences without vulnerabilities, it's a **theoretical** risk.

    - Then, if you have a vulnerability and a consequence but no threat, then you have a **cyber risk exposure**. But at any time, the threat can happen and then at this point, the cyber risk exists.

- Cyber Risk: Represents the potential for losses or damages that may occur due to a threat exploiting a vulnerability and resulting in a consequence. It is the overarching concept that encompasses all aspects of the potential negative outcomes of cyber events.
- Potential Cyber Risk: The intersection of Threat and Vulnerability, highlighting that there is a risk present if both a threat exists and the system is vulnerable to it, even if a consequence has not yet occurred.
- Theoretical Cyber Risk: The intersection of Threat and Consequence, there is a theoretical risk when a threat could have serious consequences, even if a current vulnerability isn't identified.
- Cyber Risk Exposure: This is the area where Vulnerability and Consequence intersect, indicating that there is exposure to risk when a system is vulnerable and the consequences of an exploit are potentially significant, regardless of the current level of threat.

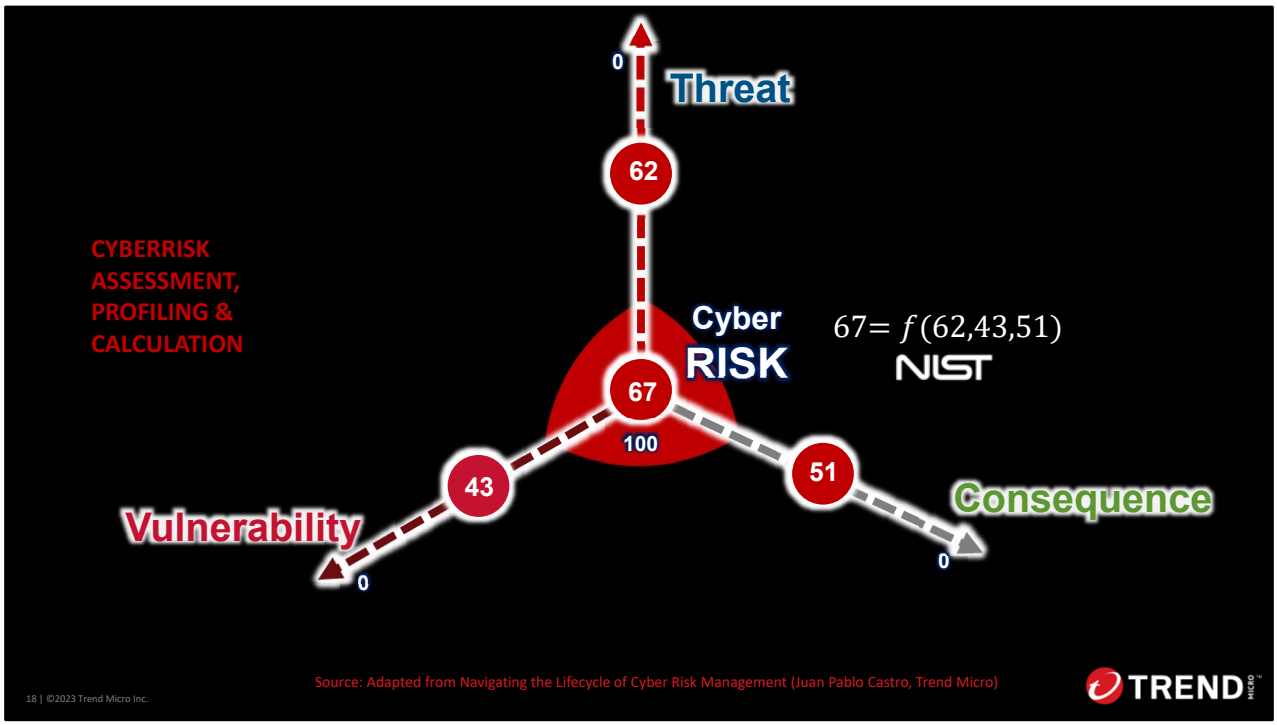
Central to the Cyber Risk Management Lifecycle is the in-depth analysis of vulnerabilities, threats, and consequences, as illustrated by the intersecting circles of the diagram. Each component plays a critical role in the formulation of an organization's cybersecurity risk index or your risk posture, and **ONLY, when all three are present does a cyber risk materialize.**

This explanation provides a qualitative understanding of the main concepts, but once we delve into calculations, the picture becomes much clearer!



To simplify the discussion about risk, instead of diving straight into complex terminology like threats, vulnerabilities, heat maps etc., consider this straightforward approach. Start out by placing your cyber risk at the center as a variable, with three axes representing threats, vulnerabilities, and consequences.

Picture the score ranging from zero at the edge to 100 at the center. Next, assign values to each component—let's call them X, Y, and Z—and then use a **formula** to calculate the overall cyber risk score.



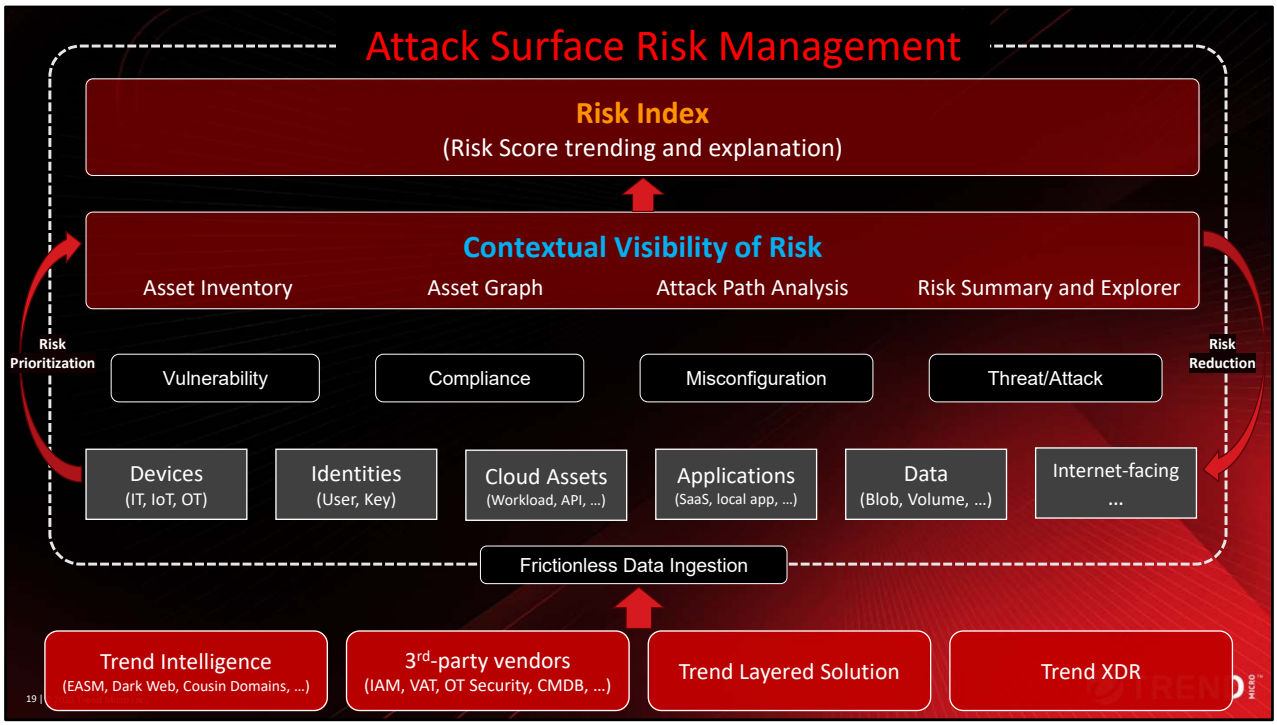
Going further we then add in some numbers. For instance, here we have a threat score of 62, a vulnerability score of 43, and a consequence score of 51, and when all this is calculated, you end up with an overall risk as 67. This numerical approach is essential, because you are starting with a value, and with values you can then compare them.

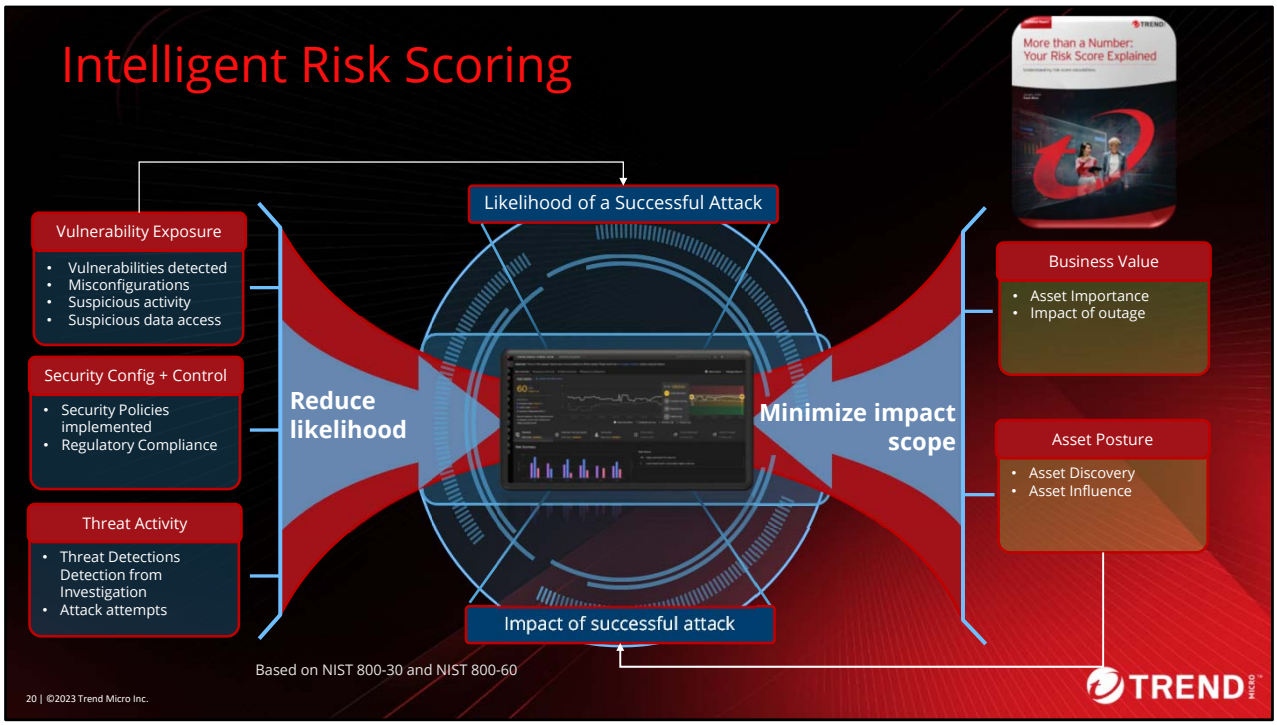
This is especially important for business leaders like CEOs or CFOs, who may not grasp what ransomware is, what the name is of the black basta family, or if something is a vulnerability, a CVE and so on, but they do understand numbers. They can easily compare numbers, and they can compare the performance of the company based on numerical values. Public companies use similar methods, like stock market comparisons, to gauge their performance against competitors.

Vision One ASRM is dedicated to solving the persistent challenge you face daily: assessing and calculating cyber risk within a dynamically evolving environment.
It is also vital to recognize that this scoring is not fixed or static. While you could manually undertake these calculations (if you so desired!), it's essential to note that these variables are continually in flux. Threats, vulnerabilities, and consequences can swiftly evolve, necessitating ongoing recalculations to proactively manage cyber risks.

In Vision One ASRM, the cyber risk calculation is a dynamic process that adapts to the evolving landscape of threats.

This example highlights the invaluable role of Vision One in managing your risk calculations. Utilizing NIST standards, Vision One ensures meticulous and reliable risk assessments, streamlining your cybersecurity efforts.


Attack Surface Risk Management
Risk Index
(Risk Score trending and explanation)
Contextual Visibility of Risk
Asset Inventory
Asset Graph
Attack Path Analysis
Risk Summary and Explorer
Risk Prioritization
Risk Reduction
Vulnerability
Compliance
Misconfiguration
Threat/Attack
Devices
(IT, IoT, OT)
Identities
(User, Key)
Cloud Assets
(Workload, API, ...)
Applications
(SaaS, local app, ...)
Data
(Blob, Volume, ...)
Internet-facing
...
Frictionless Data Ingestion
Trend Intelligence
(EASM, Dark Web, Cousin Domains, ...)
3rd-party vendors
(IAM, VAT, OT Security, CMDB, ...)
Trend Layered Solution
Trend XDR



Trend Vision One ASRM provides quick and accurate risk assessments by **continuously** updating metrics and generating individual asset risk scores and a company-wide **risk index**.
It monitors cyber assets like devices, public domains, IPs, applications, cloud assets, and identities by analyzing vulnerability, exposure, security control data, XDR telemetry, and threat intelligence feeds.

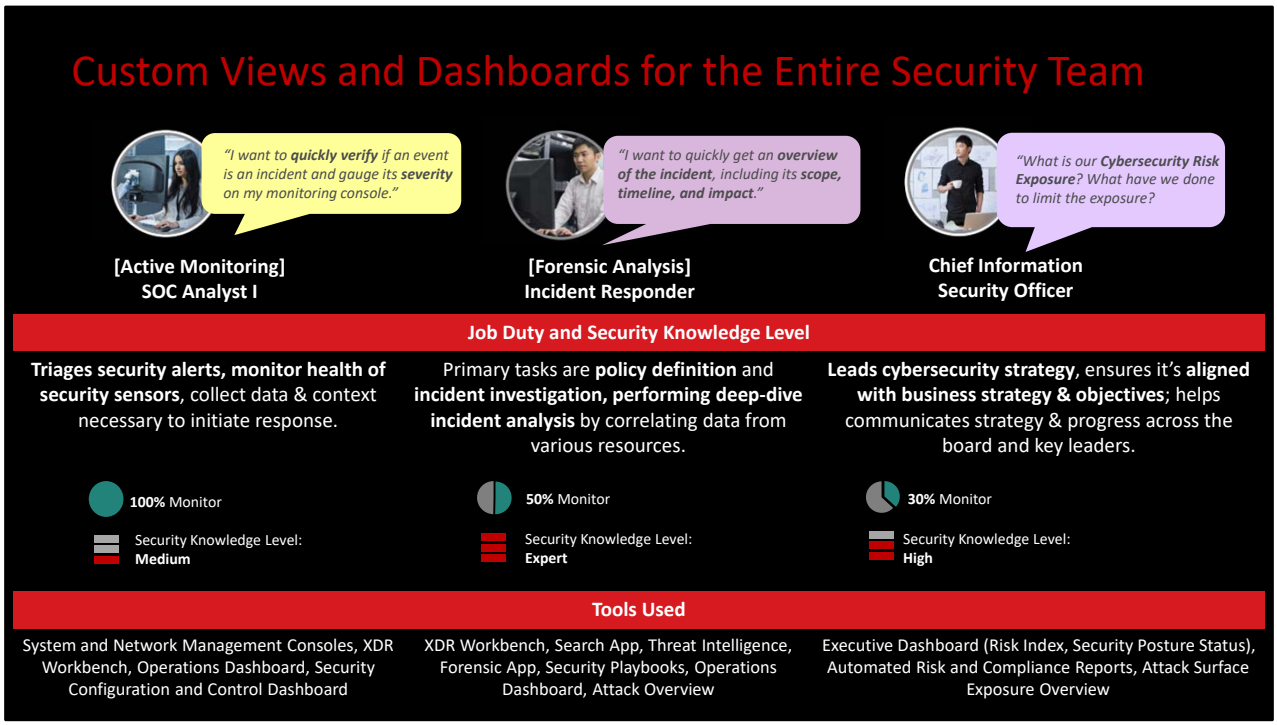
<u>Risk Calculation Brief Overview</u>

- We use standard risk management methodology starting off with **likelihood of risk** vs **impact of risk**.
- On the left we have things that go into calculating that likelihood like vulnerabilities, misconfigurations, security policies, threat detection, and attack attempts; multiply that with the criticality of the asset
- When we're assessing risk in the environment our assessment goes beyond vulnerability scans to account for security controls and configuration, threat activity as well as exposure in order to make the best decisions possible; this helps organizations:
    - Identify unpatched or misconfigured systems and risky user behavior
    - Prioritize vulnerability remediation actions and;
      Reduce potential severity of the attack
    - Inform secure remote access
- The risk index calculation, ranging from 0 to 100, enables you to make informed

decisions and prioritize risk mitigation efforts.

- The risk calculations are based on NIST 800-30 and NIST 800-60 (https://csrc.nist.gov/pubs/sp/800/30/r1/final)
- 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.

For a comprehensive understanding of our risk calculation methodology and the standards we adhere to, we invite you to explore our white paper, "More than a Number: Your Risk Score Explained." https://www.trendmicro.com/en_ca/business/products/detection-response/attack-surface-management.html?modal=s3b-btn-get-the-report-a2575b#tabs-69e2de-2



Vision One has custom views and dashboards for the entire security team, from generalist to specialist to senior leader.
This training focuses on two main persona use cases (as shown in the outside columns of this illustration)
Let's break down the key points:

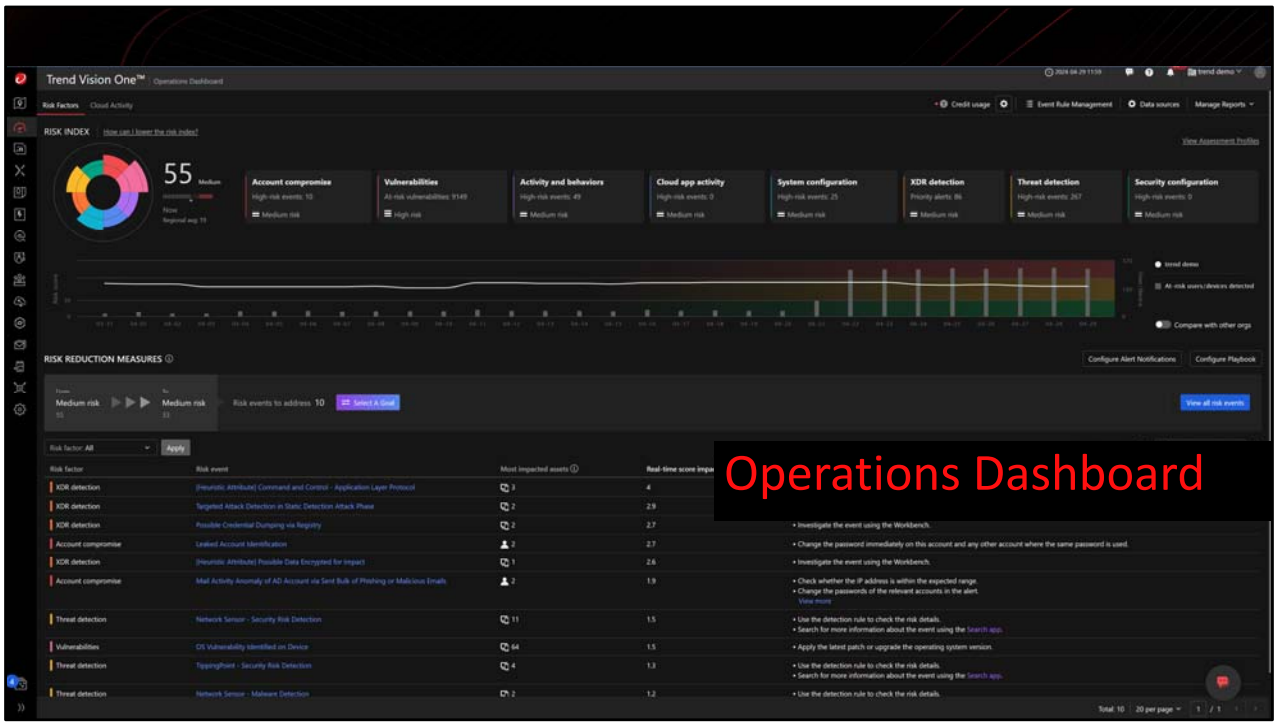
1. Personas:
    - **Operations Personas:** These include SOC Analysts, IT Operations, and others. They focus on lowering the risk score. Their main dashboard is the **Operations Dashboard**.
    - **Executive Personas:** These individuals are concerned with monitoring and reporting. They primarily work in the **Executive Dashboard**, where they review items like the Risk Index, Security Posture Status, Reports, and attack surface exposure.
2. Vision One XDR:
    - The middle column is covered by **Vision One XDR**, which will not be covered in today's session. If you're interested in learning more about XDR tools in Vision One designed for Incident Responders, we recommend checking out the Trend Education portal for XDR training.

Use the **Executive Dashboard** to get better insights into your company's security posture including the overall risk index, device exposure, and on-going attacks.

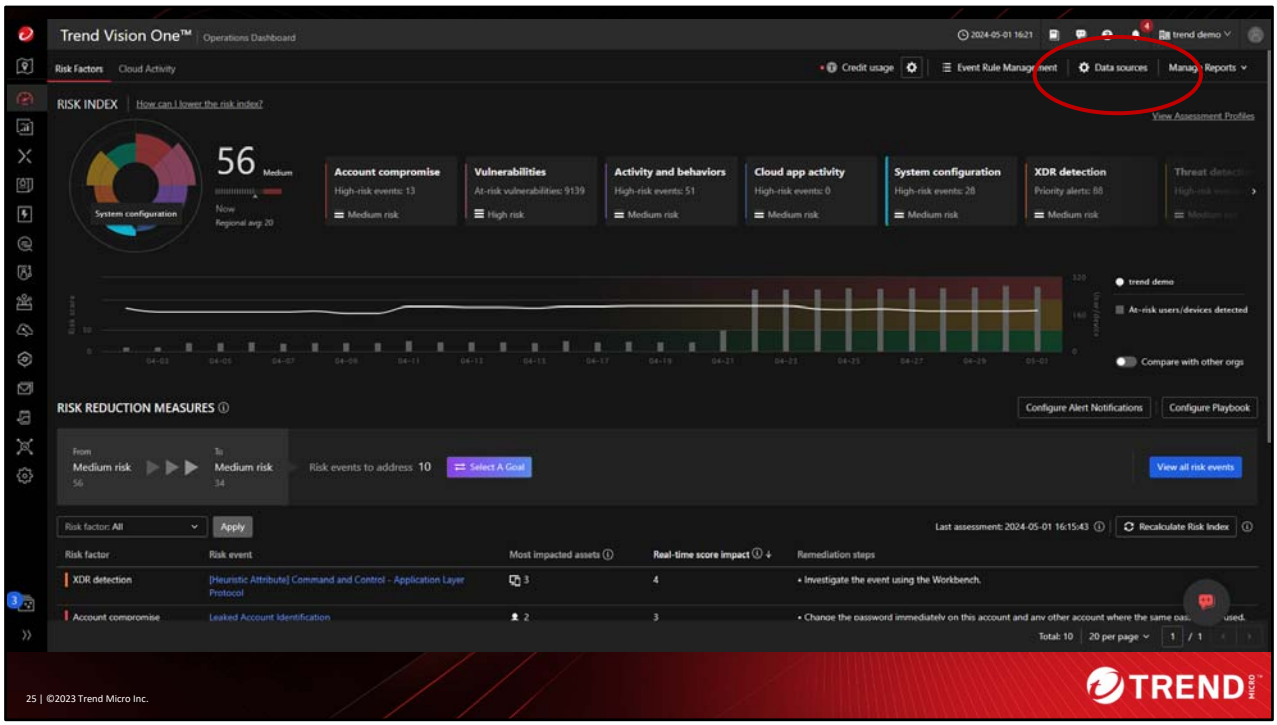
Centralized Reporting and Benchmarking

The Executive Dashboard, helps you understand and report on how risk is changing over time. Vision One aggregates data from across the enterprise, including third-party security tools, so you can identify areas of weakness, make risk-informed decisions, and benchmark against peers in the same region, industry, or company size.

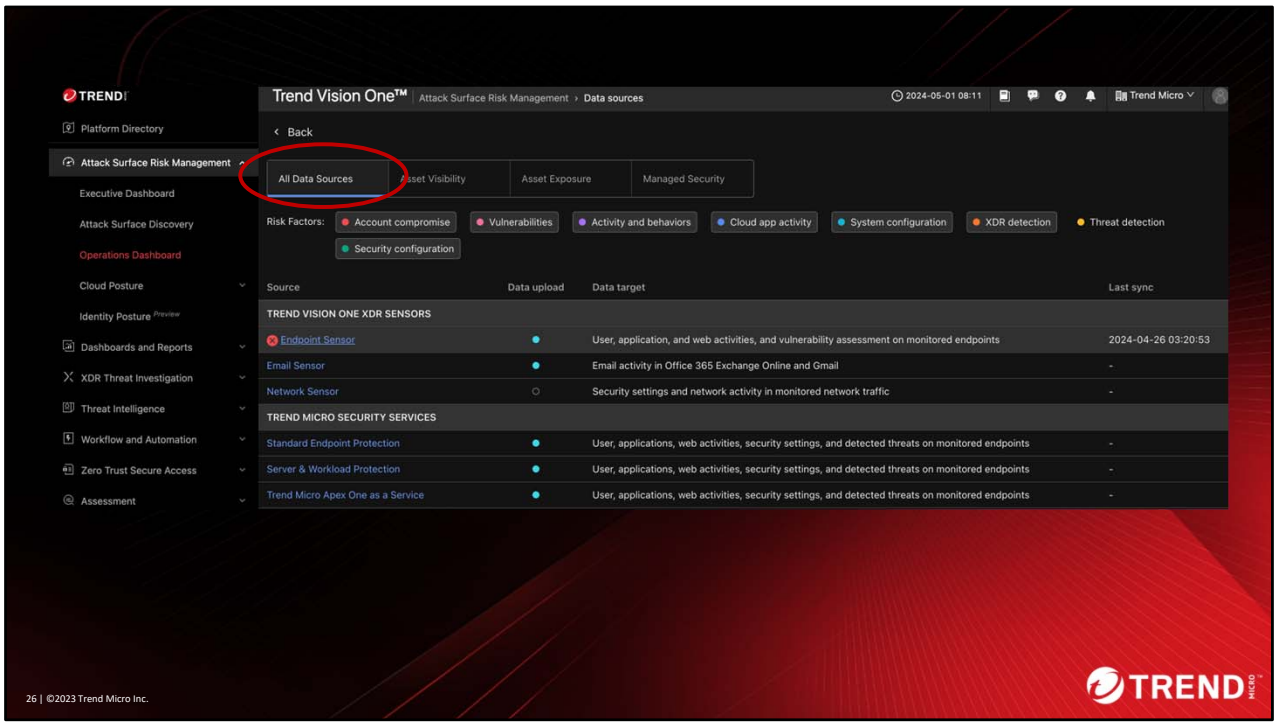
During the upcoming demo, we'll delve into the Executive Dashboard more closely.



Use the **Operations Dashboard** to implement risk mitigation actions.



Within the **Operations Dashboard**, you'll notice the following button labeled "Data sources." Note that these data sources play a crucial role in calculating your risk index. Data sources are what provide essential information for assessing and quantifying risks within your organization.



When you click the “Data Sources” button you will be able to view all the data sources that are contributing event data to Vision One.
This view provides a clear visualization of the relationship between data sources and individual risk factors. Each data source directly corresponds to specific risk factors that Vision One can identify.

On the left side, you’ll find the sources contributing data, which informs the risk factors displayed on the right.
Those blue dots represent the sources that upload event data to Vision One.
It’s evident that the greater number of blue dots you observe, the more comprehensive your understanding becomes of your organization’s security posture. Consequently, prioritize adding as many data sources as possible to improve your risk management efforts.

And now let’s jump into the demonstrations of the Executive and Operations Dashboards.

Demo: Executive and Operations Dashboard

When it comes to **risk management**, most security professionals have a single focus: **How can I reduce my risk?** It's a critical question, and organizations strive to implement effective strategies to minimize vulnerabilities, mitigate threats, and enhance their overall security posture.

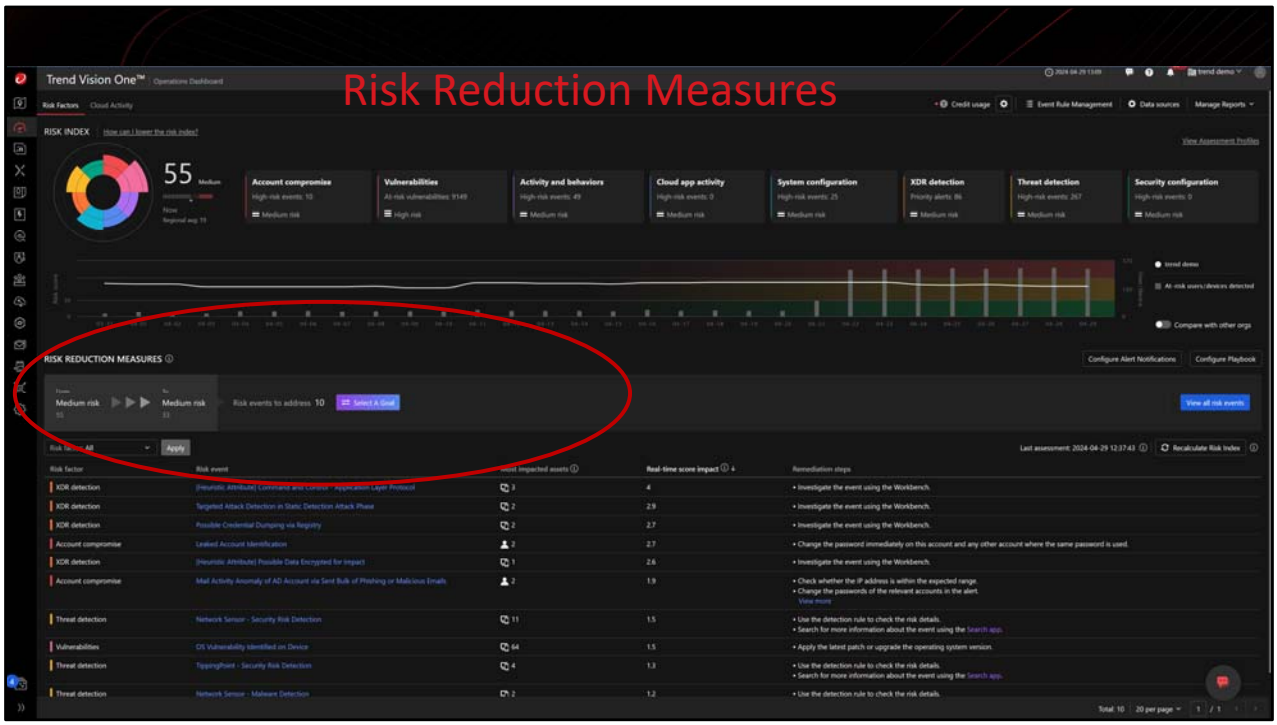
General best practices that security teams can use to achieve their risk reduction goals include:

- Set goals: What are your objectives for risk reduction? Are you simply trying to lower your current risk index? , or match the industry standard? etc.
- Prioritize risk events: It is important to manage resource allocation effectively by working on risk events that have the highest impact.
- Assess and readjust: Continuously assess risk re-adjusting your strategy as you go
- Communicate risk: Communicate your risk to risk-decision makers and stakeholders

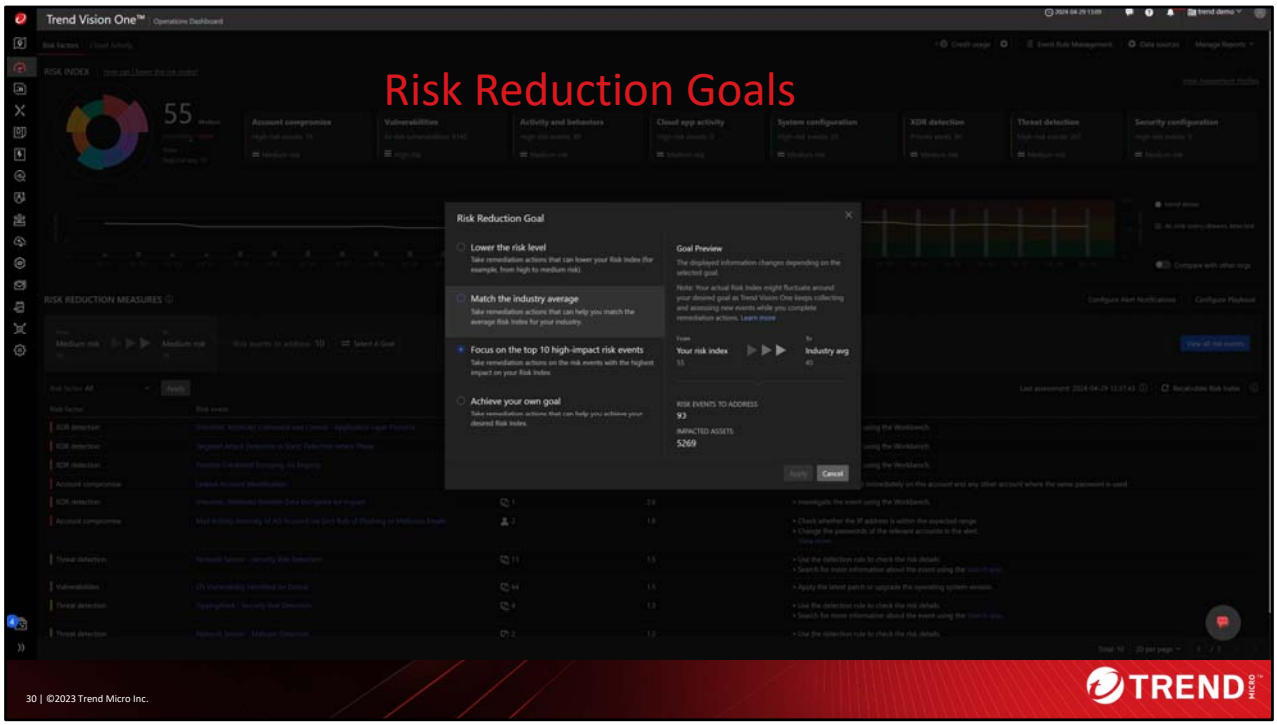
- Consider the following scenario: An IT manager observed that the top 10 risk events categorized under the "RISK REDUCTION MEASURES" were all "XDR" detections. The Managed Detection and Response (MDR) team informed the IT manager that the workbench alerts were false positives.
    - **Issue:** Although the team closed the workbench in their case management system, they neglected to close the corresponding workbench in Vision One. This oversight occurred because their standard operating procedures (SOPs) for

the managed XDR team did not include a specific process for closing false positive workbenches in Vision One.

- **Takeaway:** Even if you have a managed XDR service, as a customer, you may still be responsible for manually closing these workbenches in Vision One. It's essential to align your procedures to ensure comprehensive incident management.



When your job involves risk mitigation, your primary focus centers on implementing **Risk Reduction Measures** within the **Operations Dashboard**.
This entails proactively taking steps to lower your organization's risk index to an acceptable level.
These measures (Remediation steps) serve as your daily to-do list, already prioritized for you by Vision One, so you can focus on the events with most significant impact on your organization’s risk posture.



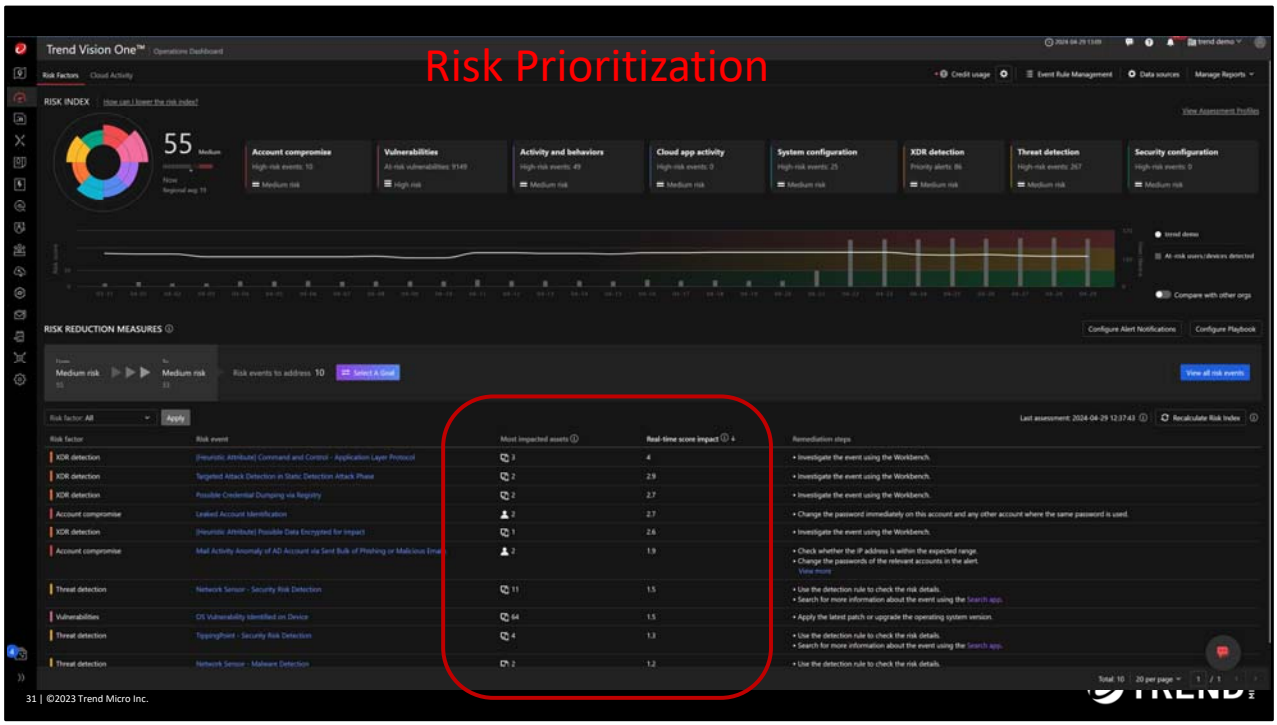
The following is the goal-setting section within the **Operations Dashboard**.
Here you decide what your risk reduction goals are.
Do you want to: Lower the risk?, Match the industry standard?, Focus on the top-10 highest risk events? Or set your own goal?
Let's take a deeper look at the functionality that is provided here:

1. Lower the Risk Level: Setting your goal to "Lower the risk level" would function as follows:
    - If you are at HIGH risk level, the events listed under RISK REDUCTION MEASURES would be adjusted to bring you down to a MEDIUM risk level
    - If you are at a MEDIUM risk level, the event listed would be aligned to further reduce your risk, taking you to a LOW risk level
    - At a LOW risk level, the focus would be on maintaining safety and preventing any potential risk exposures

    Note: Remember that risk levels are dynamic, and adjustments are made based on the prevailing situation. It is essential Stay informed and follow recommended safety measures to minimize security risks.

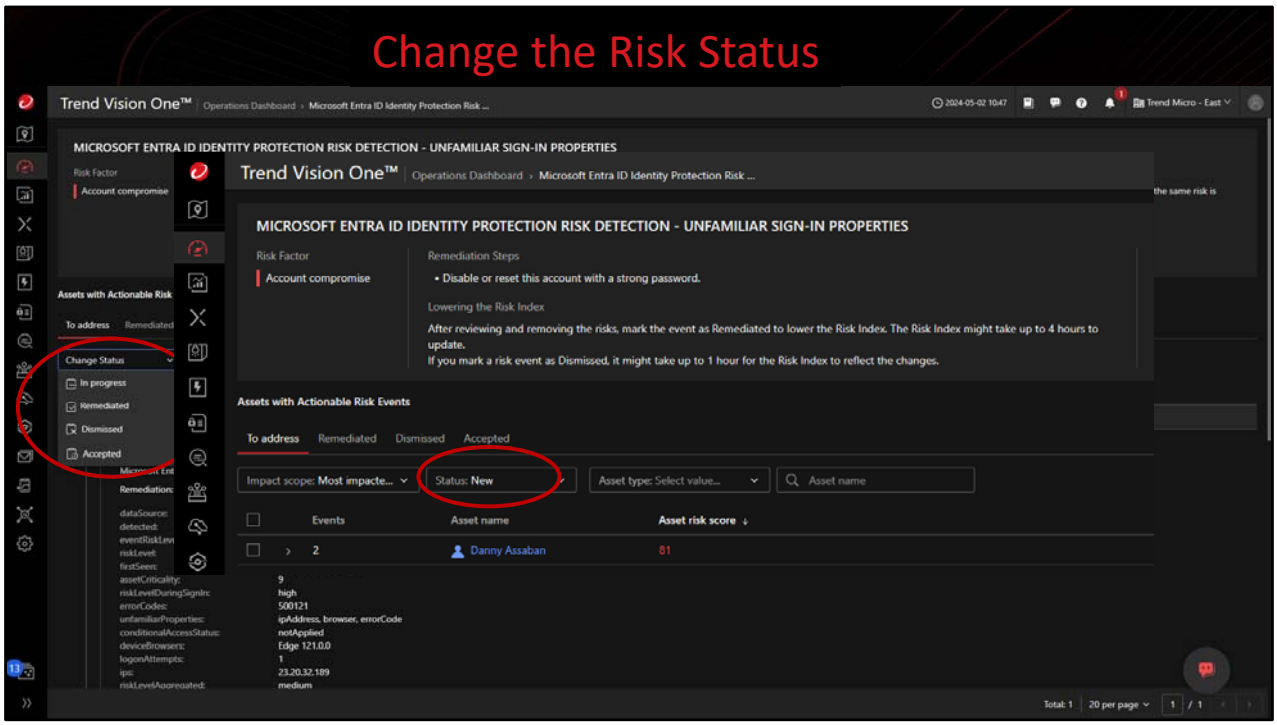
2. Match the industry average: Shows the events that you should remediate to help you match the average risk index for your industry.
3. Focus on the top 10 high-impact risk events: Shows you the events to remediate which are affecting your Risk Index the most.

4. Achieve your own goal: Set your own custom goal to achieve your own Risk Index outcome.



Risk prioritization means figuring out which risks are the most important to deal with first allowing you to:

- Use your time and money on handling risks that could cause the most harm.
- Reduce the impact of critical risks on your business.
- Enhance decision-making and clarity on how to handle risks.
- Improve your resilience to unforeseen events and disruptions.
- Better align risk management functions to business goals.



- New: Indicates that the risk has been recently identified and still requires processing. The risk status of an event remains “new” until you change it to one of these available statuses.
    - Impact on Risk Index: The risk contributes to the overall risk calculation during this phase until further assessment.
    - Use Case: Status assigned to newly discovered risks for initial evaluation.

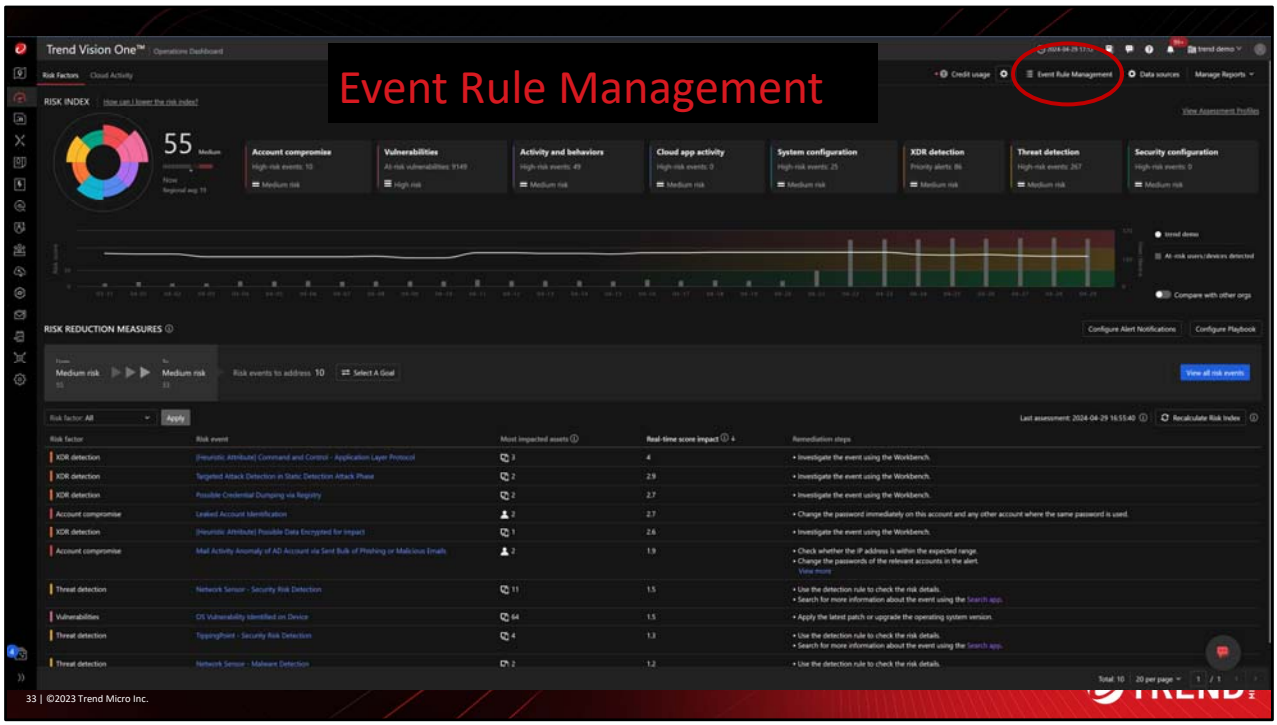
- In progress: When a risk is marked as “In Progress,” it indicates that your team is actively working on addressing it.
    - Impact on Risk Index: The risk remains part of the overall risk calculation but may be weighted less heavily during this phase.
    - Use Case: Assign this status to risks that are being investigated or undergoing processing.

- Remediated: A risk marked as “Remediated” indicates that the identified issue has been resolved or mitigated successfully.
    - Impact on Risk Index: The risk score associated with this issue decreases by the “Real-time Score Impact” value (Operations Dashboard > Risk Reduction Measures).
    - Use Case: Apply this status once the risk has been fully addressed.

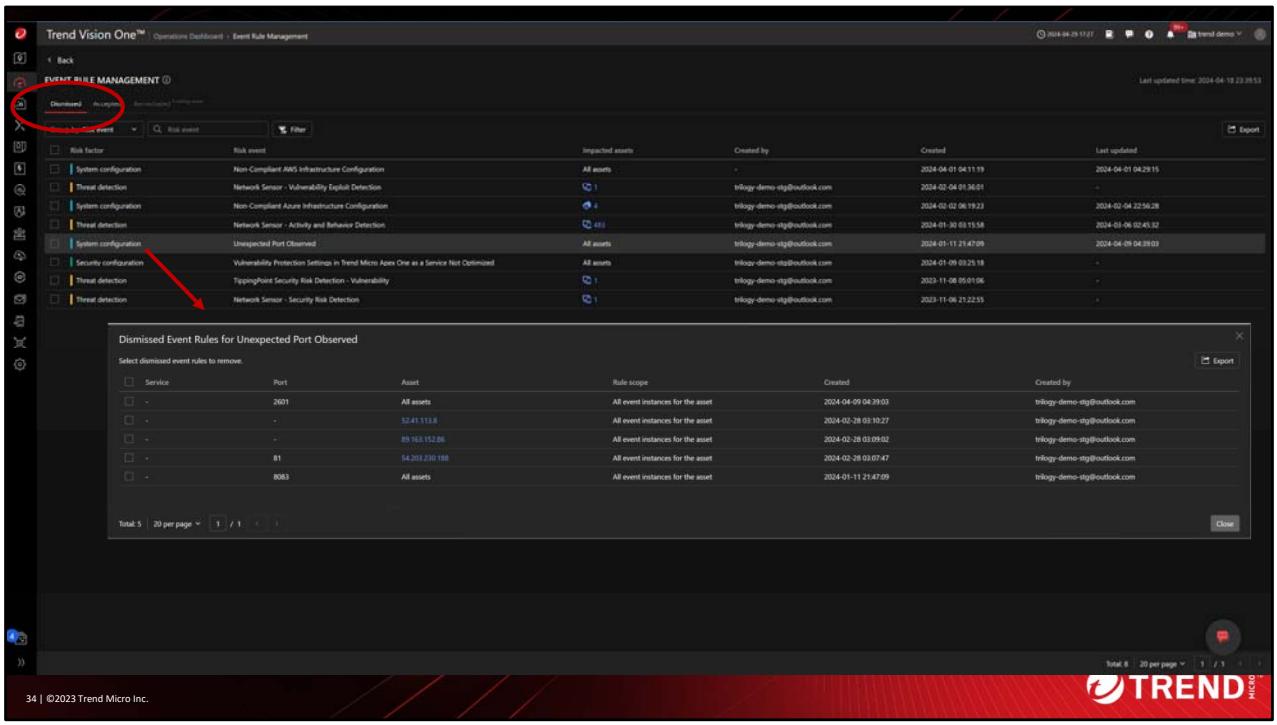
- Dismissed: Status implies that the risk was evaluated and deemed not applicable or insignificant.
    - Impact on Risk Index: Dismissed events are excluded from the overall calculation and do not affect the Risk Index until a new instance of the event is reported, or an event rule for the risk event is created.
    - Use Case: Use this status to indicate acknowledgment of a risk that you are deciding not to take immediate action (instead you are deciding to tolerate the risk temporarily). Examples include, monitoring a minor deviation, accepting a known limitation, or awaiting further data and so on.

- Accepted: When a risk is marked as “Accepted,” it acknowledges that the risk exists, but the organization has decided not to take immediate action. When marking a risk event as “Accepted”, you may create an event rule to mark current and future instances of the event as “Accepted” for a specified time period.
    - Impact on Risk Index: The risk remains part of the overall calculation. Accepted events continue to affect the Risk Index until they are remediated or dismissed.
    - Use Case: Apply this status when the risk is accepted as part of the organization’s risk tolerance. It is like saying, “I agree but I can’t do anything about it.” For example, used for events that have been marked as too difficult or expensive to address etc.

In our upcoming demo, we will provide an in-depth review of the “Change Status” options that can be used as tools for risk management.

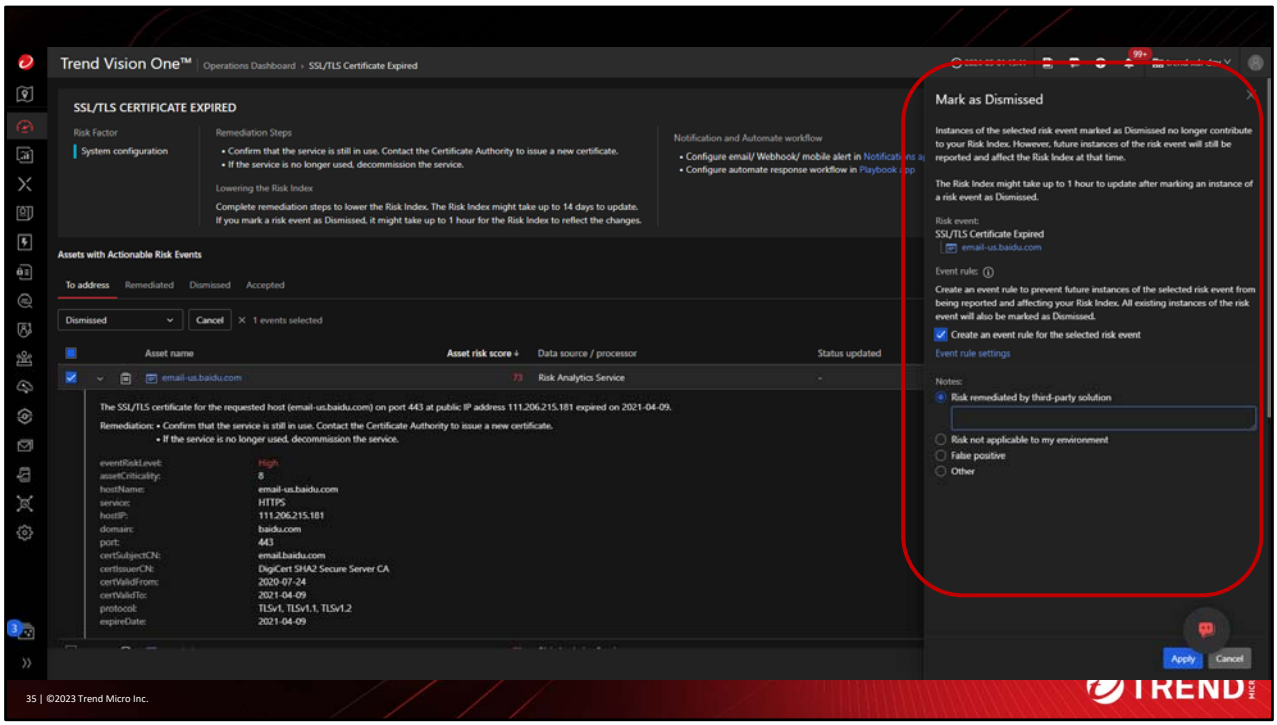


"Event Rule Management" provides a centralized location to view and manage event rules. Event rules can be created when changing the **status** of risk events to "Dismissed" or "Accepted".



Dismissed:

- Event rules for “Dismissed” events suppress the reporting of future instances of the risk event.
- Events marked as “Dismissed” will no longer negatively impact the Risk Index.

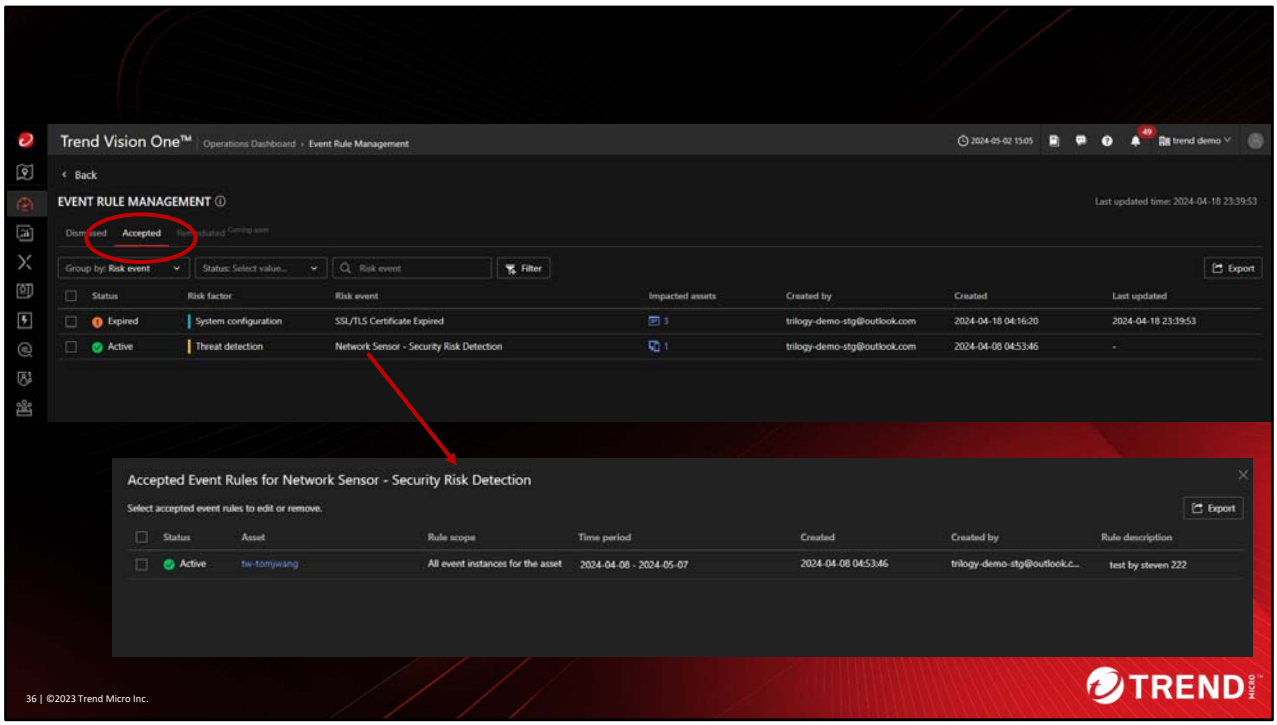


Let’s examine this functionality more closely.

Changing the event status to “Dismissed” is used to indicate that you do not agree with the event because it is not applicable to your environment.
Once you select “Dismissed”, over to the right you will have the options to create an event rule for the selected risk event. If you select this check box, you then have the option to select “Event rule settings” allowing you to specify the scope for dismissing this rule. You can select the option to apply to “All assets”, or the ones that you select.

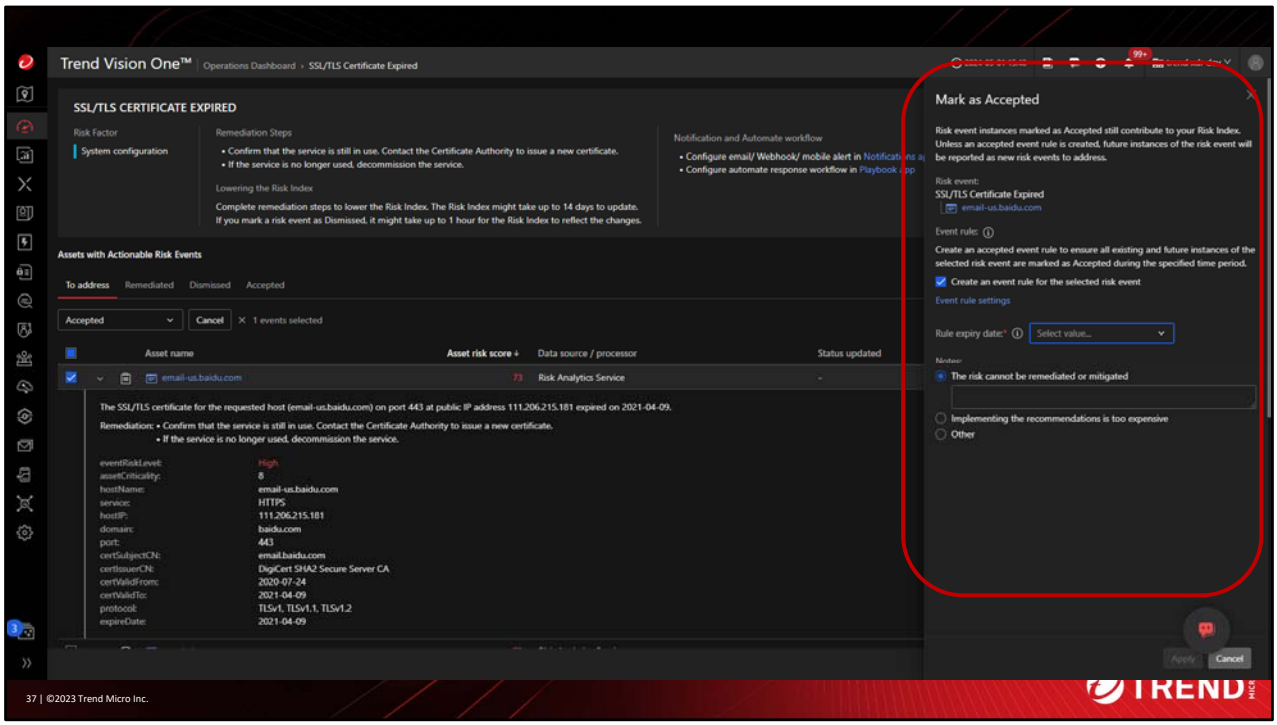
Note: By creating the event rule for the event, you are preventing duplicate events from being created in the future and clogging up your Operations Dashboard > RISK REDUCTION MEASURES which is effectively your risk (reduction) management workspace.

Under the “Notes” area on the right hand-side of the screen, you can optionally select “Risk not applicable to my environment”, “False positive” and “Other”.
This will be explored in more detail in an upcoming demo.

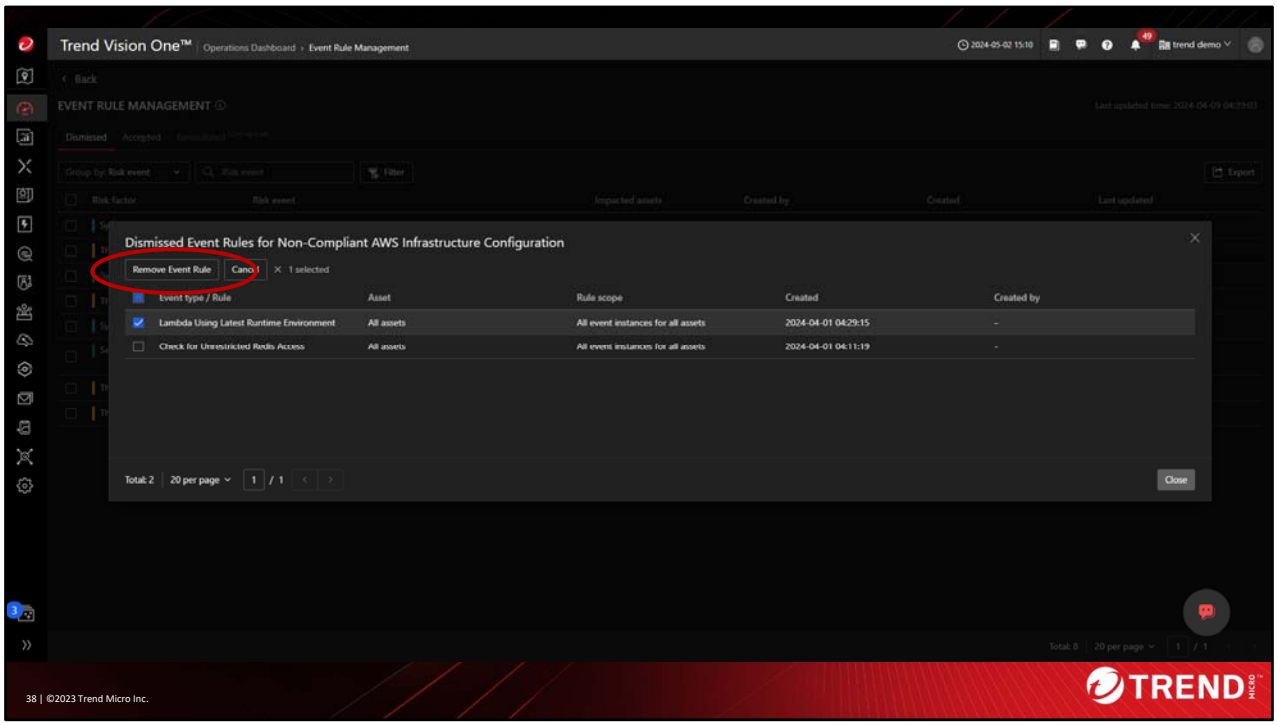


Accepted:

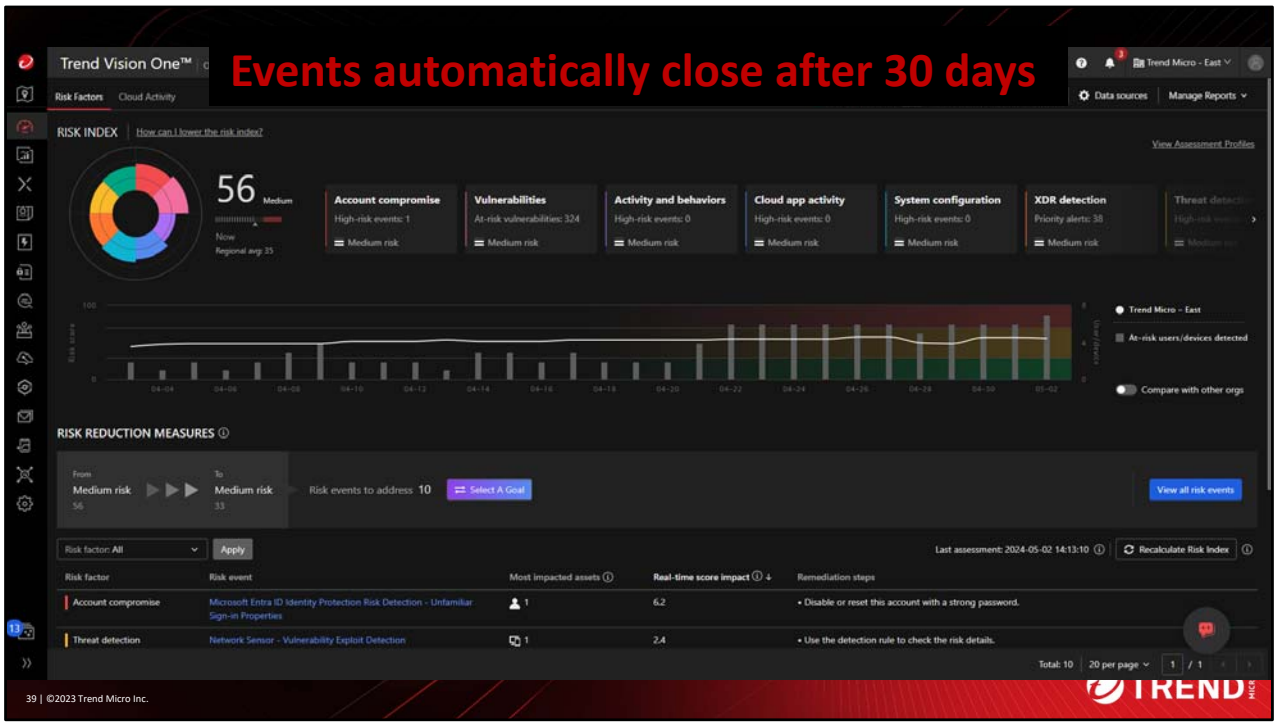
- Marking a risk event as “Accepted” and creating a related event rule ensures existing and future instances of the risk event are marked as “Accepted” for the specified time period.
- Events marked as “Accepted” will still contribute to your Risk Index.



Future instances of the selected risk event are marked as “Accepted” during the specified time period that is configured here.
You can additionally specify why the risk was accepted by selecting one of the options appearing under the “Notes” section.



Removing an event rule (in the case of false positives) provides the option for you to enable reporting for future instances of the related risk event.



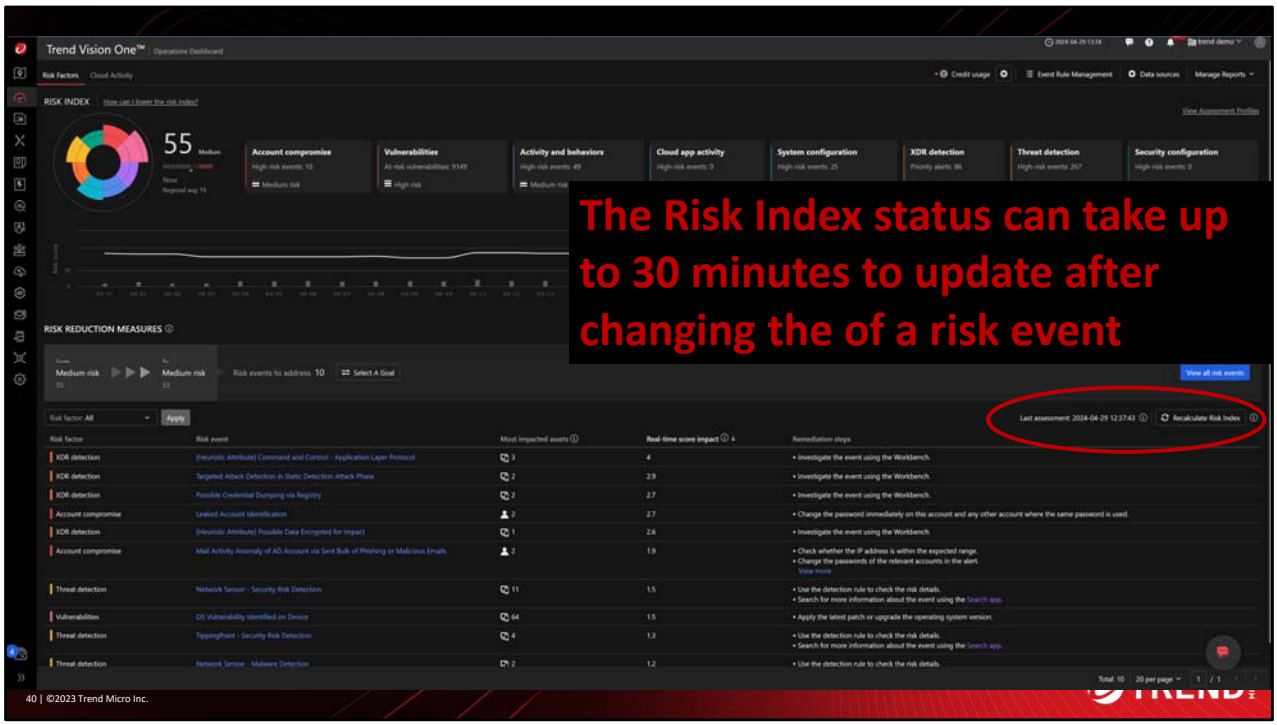
Event Autoclose Behaviour

What you are seeing here in the **Operations Dashboard** is six months of trend data. When we are looking at the events contributing to the overall risk score, for example, “56”, or whatever that number may be, it’s crucial to focus on the **Operations Dashboard**. Why? Because events automatically close after 30 days.

Consider the following scenario:

You encounter an account compromise event related to leaked account identification (with a score of two). It arrives on the 1st of the month, but no one takes action. By the 1st of the next month, that event will have automatically closed and dropped off—it’s out of the risk index and no longer part of risk reduction measures.

However, it is important to understand here that while the risk score decreases due to automatic closure, the risk itself isn’t fully remediated. It is still lurking, waiting to resurface. That’s why understanding the autoclose behavior is essential. Don’t fall into the trap of checking the dashboard only once a month. Regular monitoring ensures you don’t miss opportunities to actively manage your risk.



Assess and Readjust

After completing your risk reduction measures for the day, take the following steps:

1. Remediation Actions: Address any identified risks by taking appropriate remediation actions.
2. Recalculate Risk Index: Wait for the recalculation of the risk index or use the “Recalculate risk index” button to reassess and recalculate your risk index.
3. Adjust as Needed: Based on the updated risk score, make any necessary adjustments to manage risk effectively.

Recalculating the Risk Index: Not as Simple as a Button Press

At first glance, you might assume that clicking a button would instantly update the risk score. However, the reality is more intricate. Behind the scenes, a complex series of steps involving multiple back-end technologies comes into play. As a result, recalculating the risk index can take up to an hour. (The button is intentionally limited to run the calculation process once per hour!)

- If you’re a patient person, rest assured that the risk index will automatically adjust itself over time. But if you’re feeling impatient and want quicker results, go ahead and use the button.

Please note the following limitation: Currently, the “Recalculate Risk Index” button does

not grey out after you've clicked it. However, this issue will be resolved in an upcoming release. Once fixed, the button will correctly grey out and present a notification indicating that this state lasts for an hour. This enhancement is designed to prevent customers from repeatedly clicking the button and causing a backlog of requests on the backend. It's essential to keep in mind that when the queue gets longer, risk indexes take longer to recalculate.

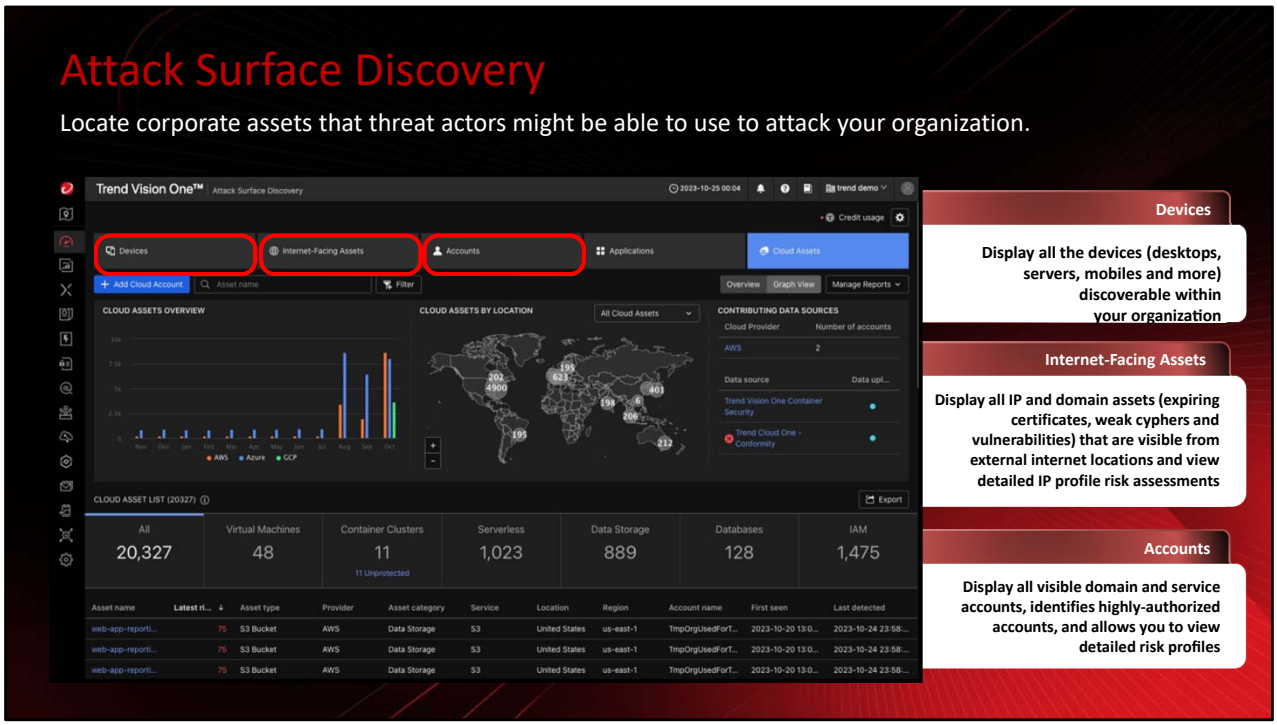
Lastly, as the risk score fluctuates, it's crucial to maintain vigilance and stay on top of timely monitoring for effective risk management.

Strategic Use of Risk Status Options:

- **Balancing Act:** Organizations should strike a balance between addressing risks promptly and managing resource allocation effectively.
- **Prioritize risks:** Prioritizing risks is a critical aspect of effective risk management. As a general guideline, prioritize risks based on severity, potential impact, and available resources.
- **Regular Review:** Regularly review risk statuses to ensure they align with the current risk landscape. Adjust status as needed based on changes in risk exposure or organizational priorities.
- **Communication:** Transparently communicate risk status changes to relevant stakeholders. Ensure that decision-makers understand the implications of each status option.

Remember that effective risk management involves **continuous** monitoring, assessment, and adaptation.
By leveraging the "Change Status" tool wisely, you can optimize your risk score and enhance your organization's security posture.


TREND MICRO
8%
80
1000
Jane Cooper
TW Jane Cooper
Darrell Steward
John Ruiz Macbook Pro
Robert Fox
TW Jane Cooper
Demo: Understanding you Risk, How to Lower your Risk Index



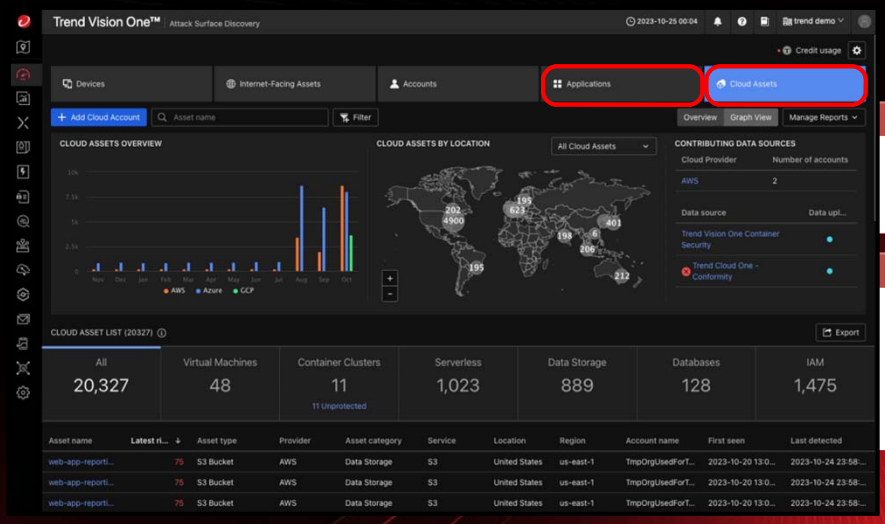
Attack Surface Discovery in ASRM offers a comprehensive asset-based view for managing your attack surface.

Here's how it helps:

1. Asset Identification: Discover all assets, both managed and unmanaged, before potential attackers do.
2. Comprehensive View: Construct a detailed picture of your attack surface using native data sources and third-party integrations.
3. Detailed Asset Profiling: Provides granularity to help you understand the impact of selected assets on your organization's overall surface risk.
4. Attack Paths: Visualize predicted attacker behavior through attack paths.

Attack Surface Discovery

Locate corporate assets that threat actors might be able to use to attack your organization.

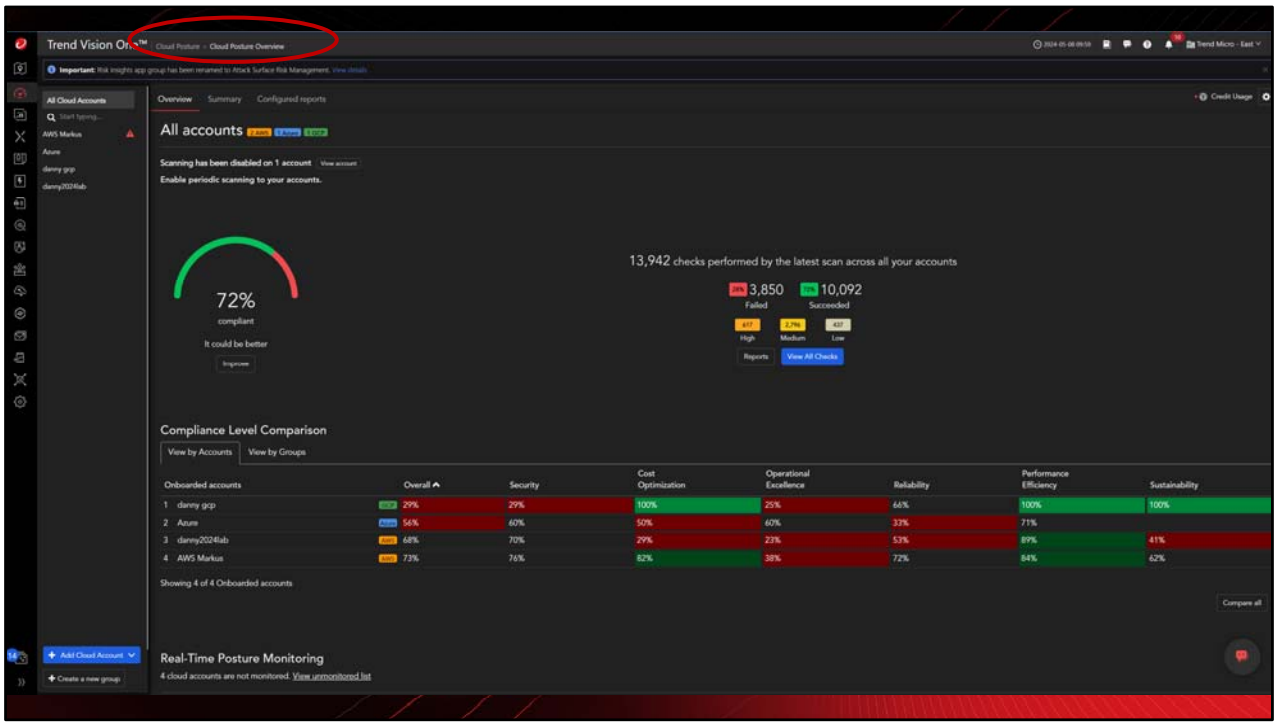


Applications

Display all the applications deployed to your devices and the cloud apps being accessed by your users.

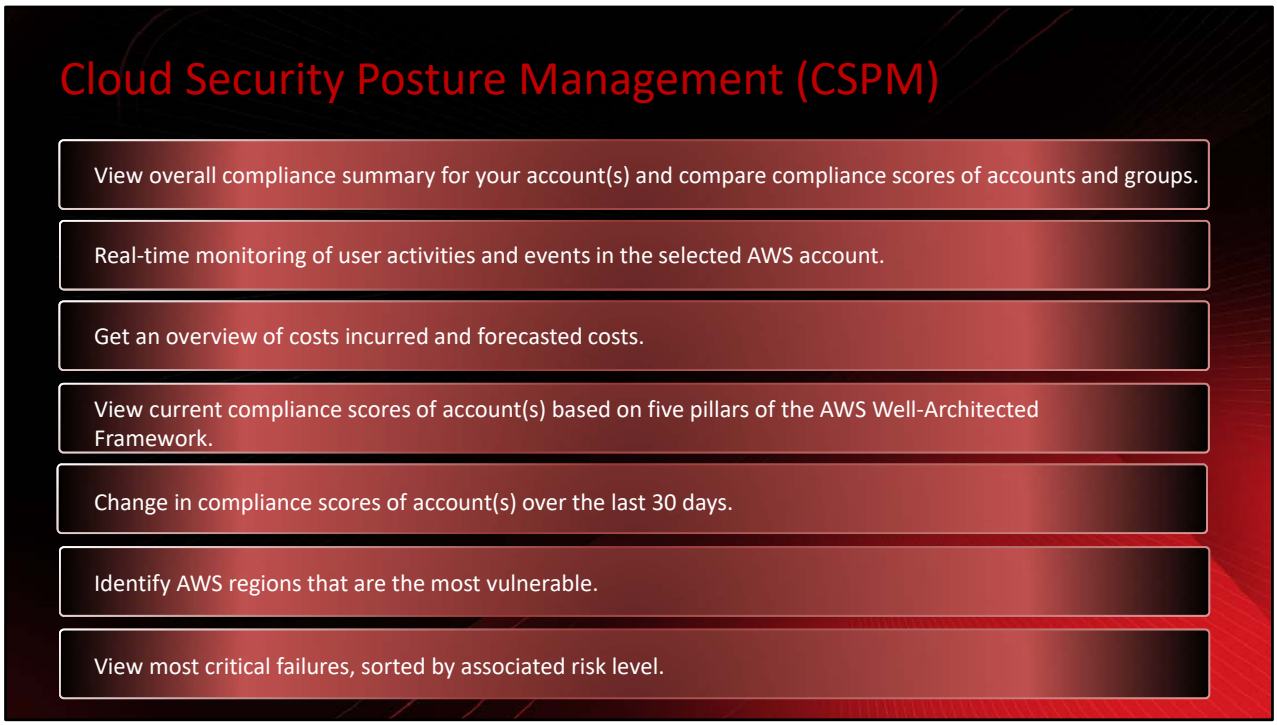
Cloud Assets

Display detected cloud resources within your organization, enabling you to rapidly identify compliance and security best practice violations on your public cloud infrastructure and across your cloud service platforms.

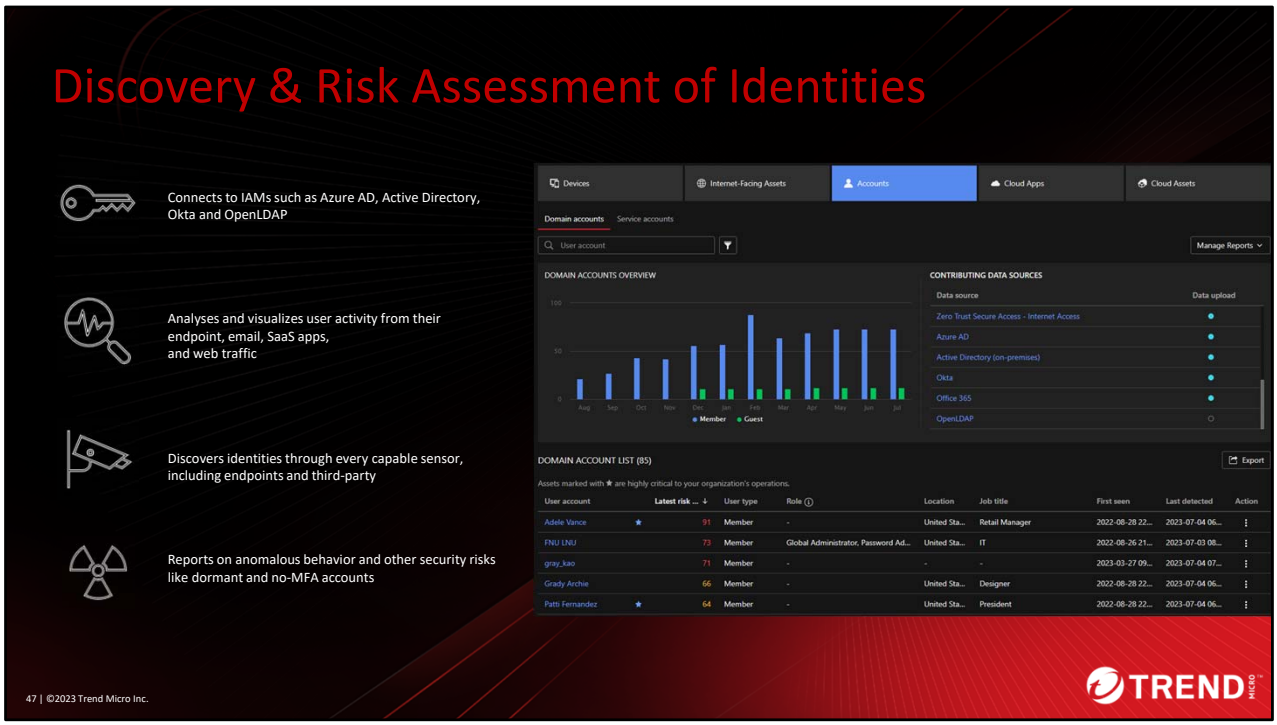


Cloud Security Posture Management

Use **Cloud Posture > Cloud Posture Overview** in Attack Surface Risk Management to display detected cloud resources within your organization, enabling you to rapidly identify compliance and security best practice violations on your public cloud infrastructure and across your cloud service platforms.



Why is having Cloud Security Posture Management important for Attack Surface Risk Management? It secures your complex hybrid cloud environment by providing security for preferred cloud platforms like AWS, Microsoft Azure, and Google Cloud Platform.

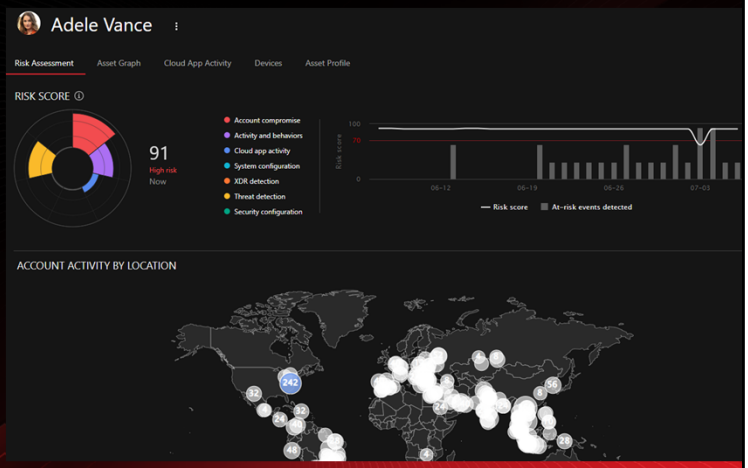


With the complexity of today's attack surface, it has also become increasingly important to understand identities and their behaviors.

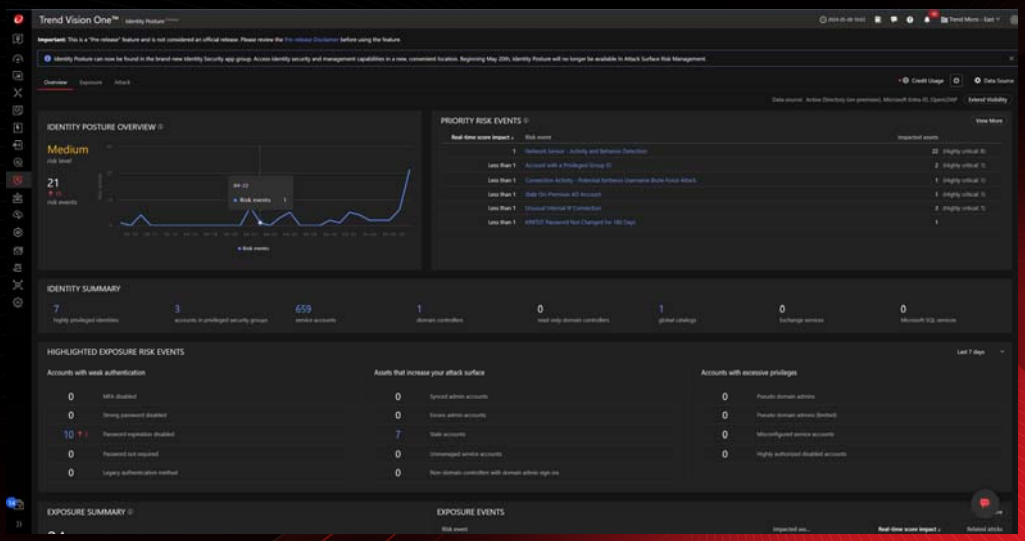
In-Depth Identity Profiles

Answering questions such as:

- How risky is this identity?
- Why are they risky?
- How has this risk changed over time?
- Where are they logging in from?
- What risks and threats have been identified?
- Who and what does this identity interact with?
- What are their common behaviors?



Identity Posture Management (in Preview)



Coming soon in ASRM is Identity Posture Management. It is currently available in Vision One in “preview” mode.


TREND MICRO
8%
80
1000
Jane Cooper
TW Jane Cooper
Darrell Steward
Robert Fox
John Ruiz Macbook Pro
Demo: Attack Surface Discovery, Cloud Security Posture Management (CSPM)

Third-Party Integration

Integrate data from various sources (for example, threat intelligence feeds, vulnerability management systems, SIEMs etc.) to create a comprehensive risk picture.

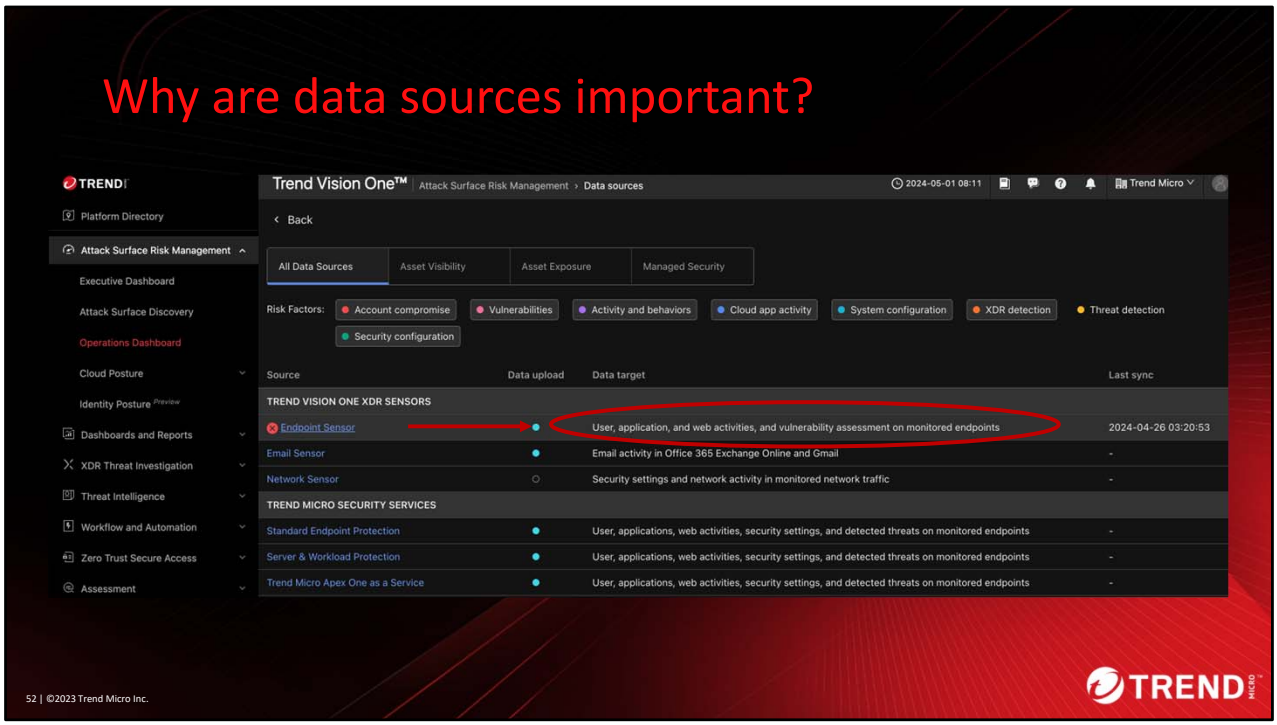
This enables ARSM to continuously query the Vision One platform for updates on asset statuses and associated risk scores.

We continue to grow our integration ecosystem to ensure Vision One fits seamlessly within your existing security stack.

Our hybrid approach stands out by extending third-party integrations to ingest and normalize activity from more of the customer environment through purpose-built and flexible API-driven integrations.

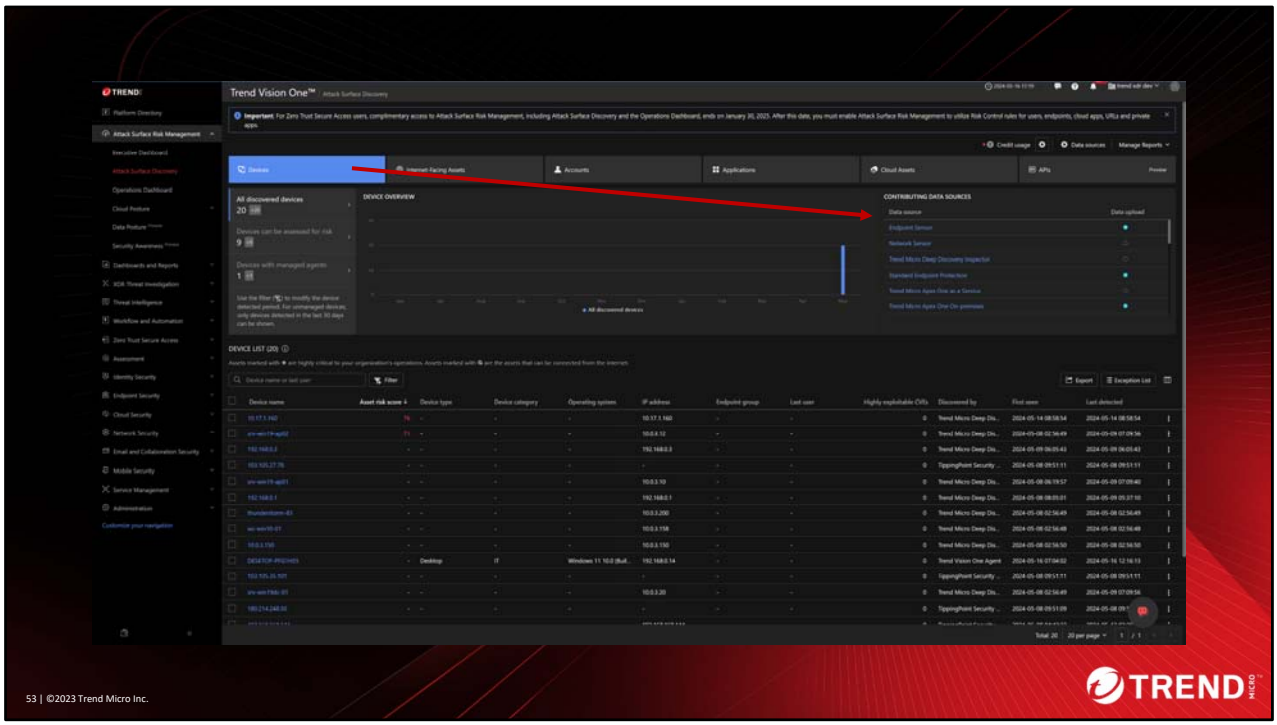
- Security Information and Event Management (SIEM)/Security Orchestration, Automation, and Response (SOAR)
- IT Service Management (ITSM)
- Breach Attack Simulation
- Managed Detection and Response (MDR)
- Cloud Services
- Threat Intel
- Network
- Endpoint Management
- Identity and Access Management (IAM)

- Vulnerability Management

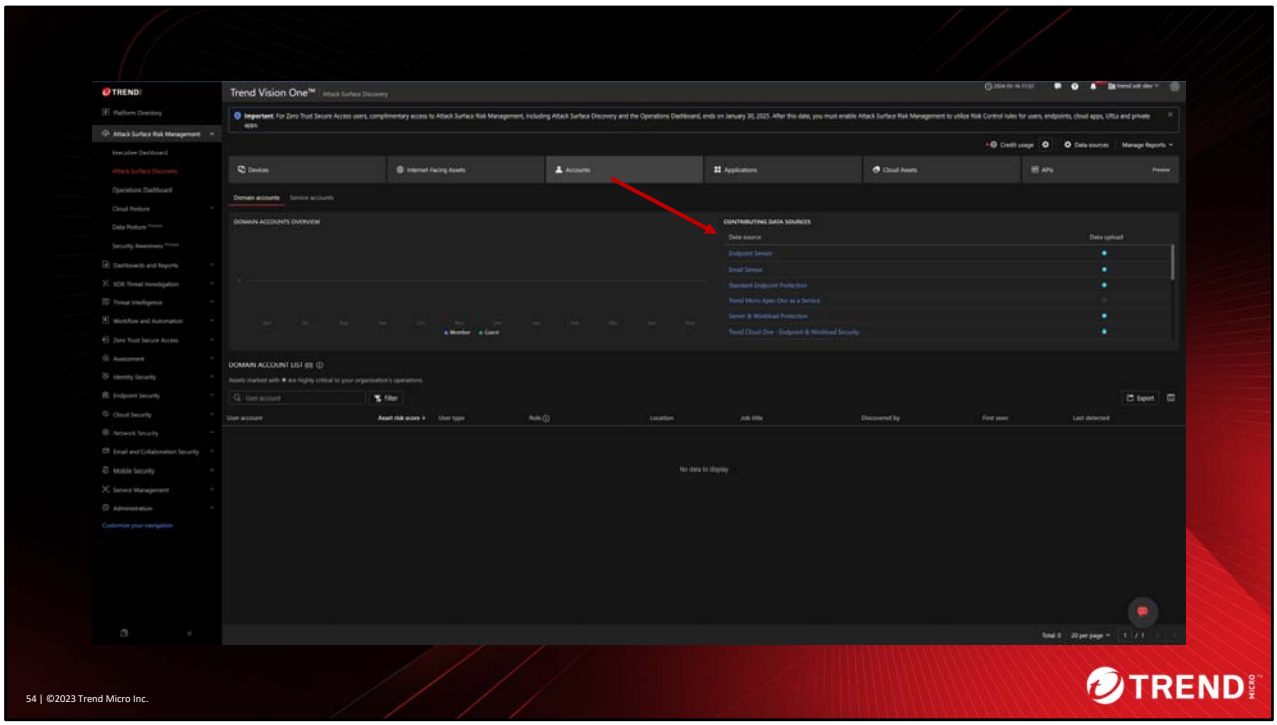


Relationship Between Data Sources and Risk Index

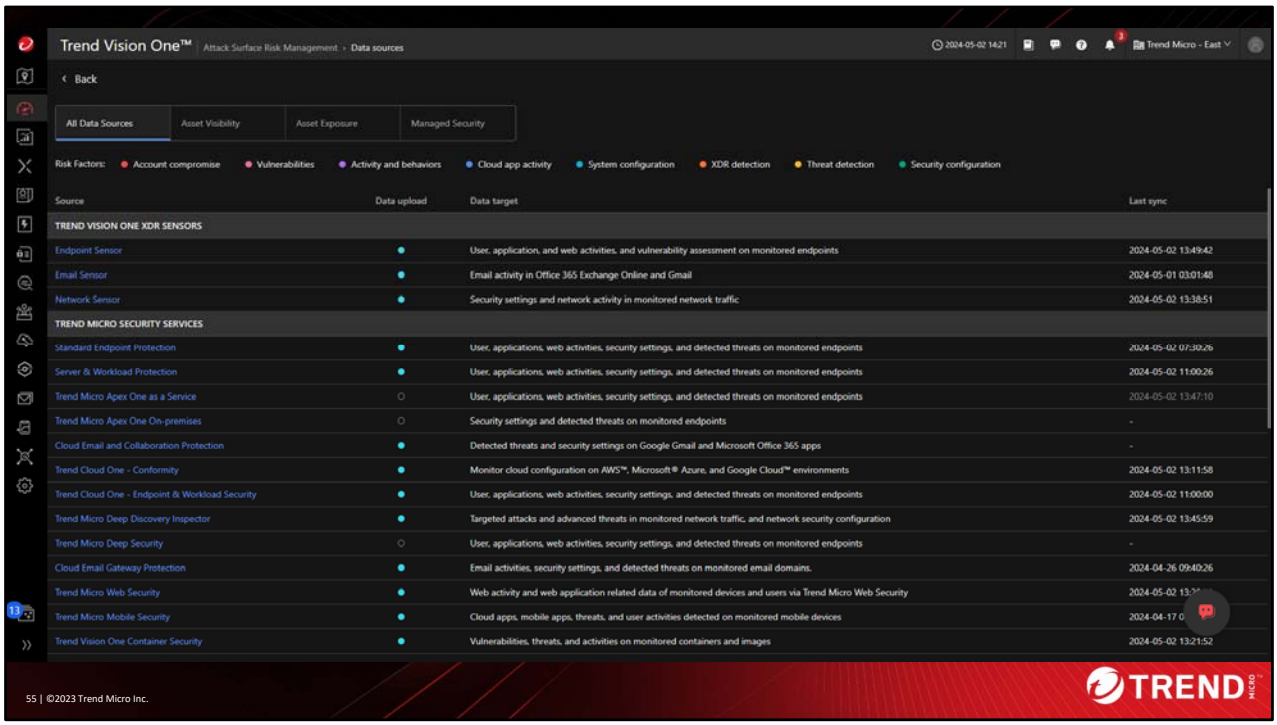
Data sources are essential for Vision One to more accurately identify, assess, and calculate risks. Each data source is directly related to specific risk factors that Vision One can identify. On the left side, you can see the sources contributing data, which informs the risk factors displayed on the right.



Another way to view data source information is as follows, by asset type.
For example, the risk factors for your “devices” are determined using the following data sources, Endpoint sensor, Standard Enpoint Protection, as indicated by the blue dot under “Data upload”. This list also identifies other data sources that you could be adding. The more data sources you connect, the more risk that Vision One is able to assess.



Here is another example, viewing data sources information for “Accounts”.



Feed data from all deployed security products into Vision One for a consolidated risk assessment.
More data sources enhance the quality and depth of risk assessment, resulting in a more accurate and complete risk score calculation.

Key points to understand the relationship between data sources and events:

Risk Index and Comprehensive Review:

- Trend Micro Vision One aims for a comprehensive review of risk in your environment, not limited to Trend Micro products alone. While Trend Micro products provide value, the real benefit lies in integrating third-party data sources. These external sources enhance the overall risk assessment.
- Consider scenarios like account compromise events or brute force password attacks. Smaller organizations may overlook these events, but connecting third-party data sources allows us to consolidate risk across different products.

Visibility and Risk Assessment:

- The more data sources you connect, the more complete your risk posture becomes. However, be aware that adding new data sources can increase your risk. Why? Because greater visibility into your environment enables better risk assessment.

IMPORTANT: If you do not see any blue dots, it indicates that you will not receive events from the corresponding security products deployed in your environment. Ensuring proper data integration is essential for effective risk assessment and comprehensive visibility.

ASRM and Third-Party Integration:

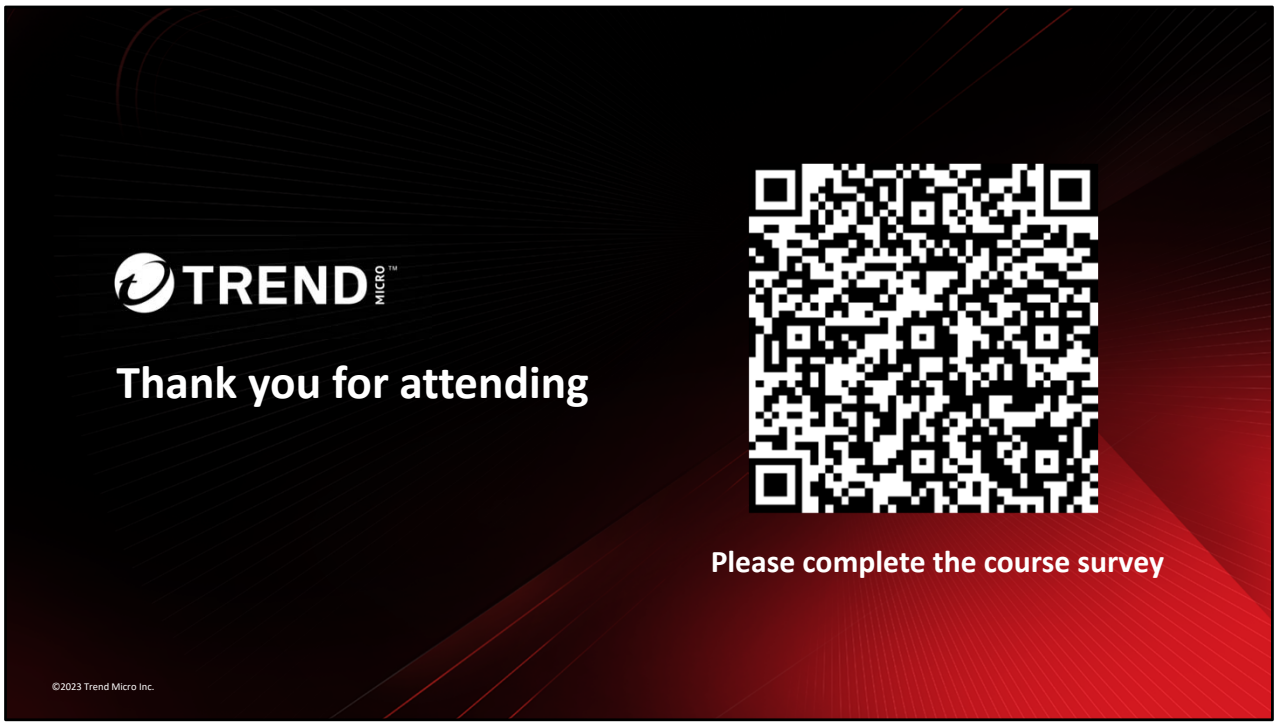
- ASRM can serve as an entry point in the area of Attack Surface Discovery. It can be deployed independently of Trend Micro products and offers the potential to integrate various third-party data sources.
- Trend Micro's ongoing integration projects with different companies demonstrates the significance of extending the ecosystem.
- Vision One's impact: Vision One is transforming SIEM (Security Information and Event Management) for many organizations.

Demo: Third-Party Integration and Data Sources

Review and Key Takeaway!

- Attack Surface Discovery Challenges
- Trend Vision One ASRM
- Risk Index Calculation
- Executive and Operations Dashboard
- Risk Prioritization
- How do I lower my risk?
- Attack Surface Discovery
- Cloud Security Posture Management
- Third-Party Integration
- Data Sources

A 30-day full access trial of Trend Vision One is available for download.



Please complete the class survey at the following URL or by scanning the QR code:
https://www.surveymonkey.com/r/TrendMicroVisionOne

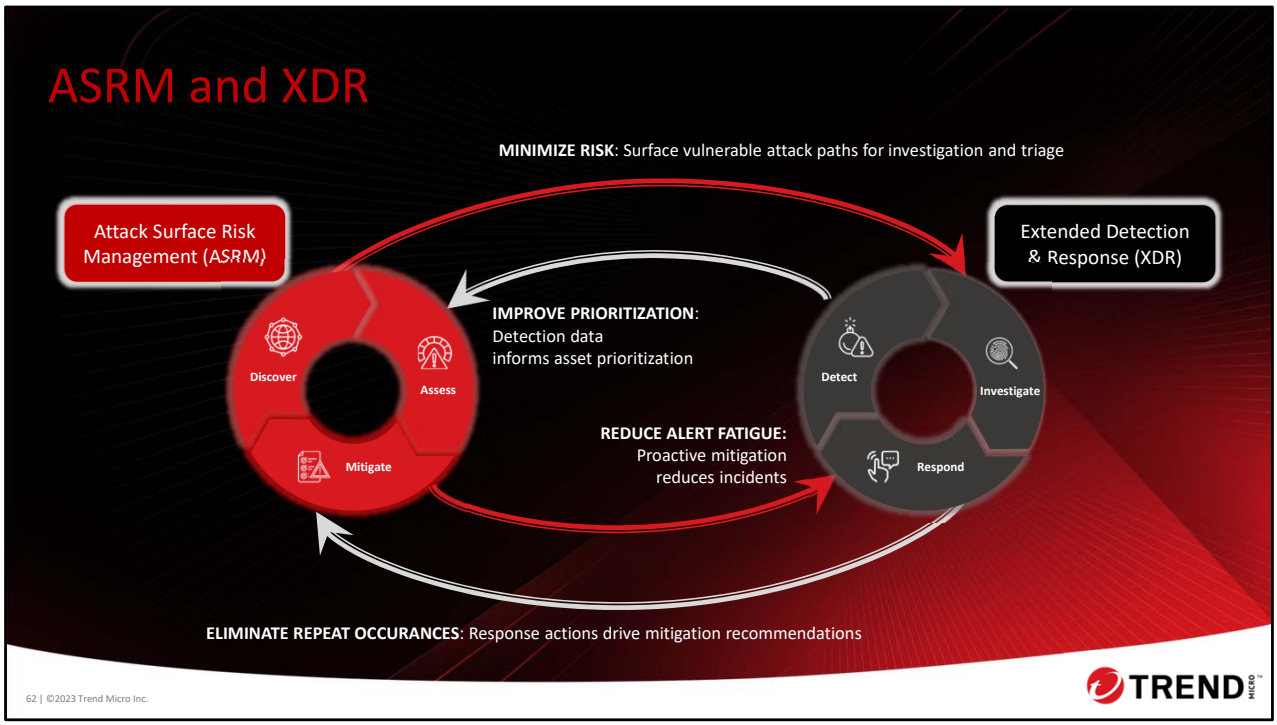
This helps guide the development of courses and helps ensure that content matches your requirements.

Thank you for attending.

Additional Resources

- Trend Vision One™: The Power of your Risk Score
  - https://youtu.be/EEfP-AqPILY?si=Ho9O7XXmMCL1ZPs0
- Attack Surface Risk Management - Take Charge of Risk (Demo)
  - https://youtu.be/cknqj0strTk?si=fkvpixAkfbs6nFNA
- Attack Surface Risk Management - Actionable Insights (Demo)
  - https://youtu.be/myOks054mR0?si=uQlwZySwC98cBMvU
- MORE THAN A NUMBER-YOUR RISK SCORE EXPLAINED.pdf
  - https://resources.trendmicro.com/rs/945-CXD-062/images/MORE%20THAN%20A%20NUMBER-YOUR%20RISK%20SCORE%20EXPLAINED.pdf
- For more learning resources visit: Education.trendmicro.com


Appendix
TREND



As you can see, whether we are talking about a CISO managing risk or a SOC leader trying to respond to threats, the challenges are related.

- The more proactive risk mitigation, the fewer security incidents the SOC team has to respond to.
- Likewise, the detection data collected by XDR provides valuable insight that can factor into risk assessments.
- There are multiple points of interaction across these functions.

This provides you with a single place where teams can work across their borders to **close the gap** between attack surface risk management and detection and response. This is the winning formula for security teams across industries.