The Defenders

How cybersecurity professionals are fighting back against threat actors

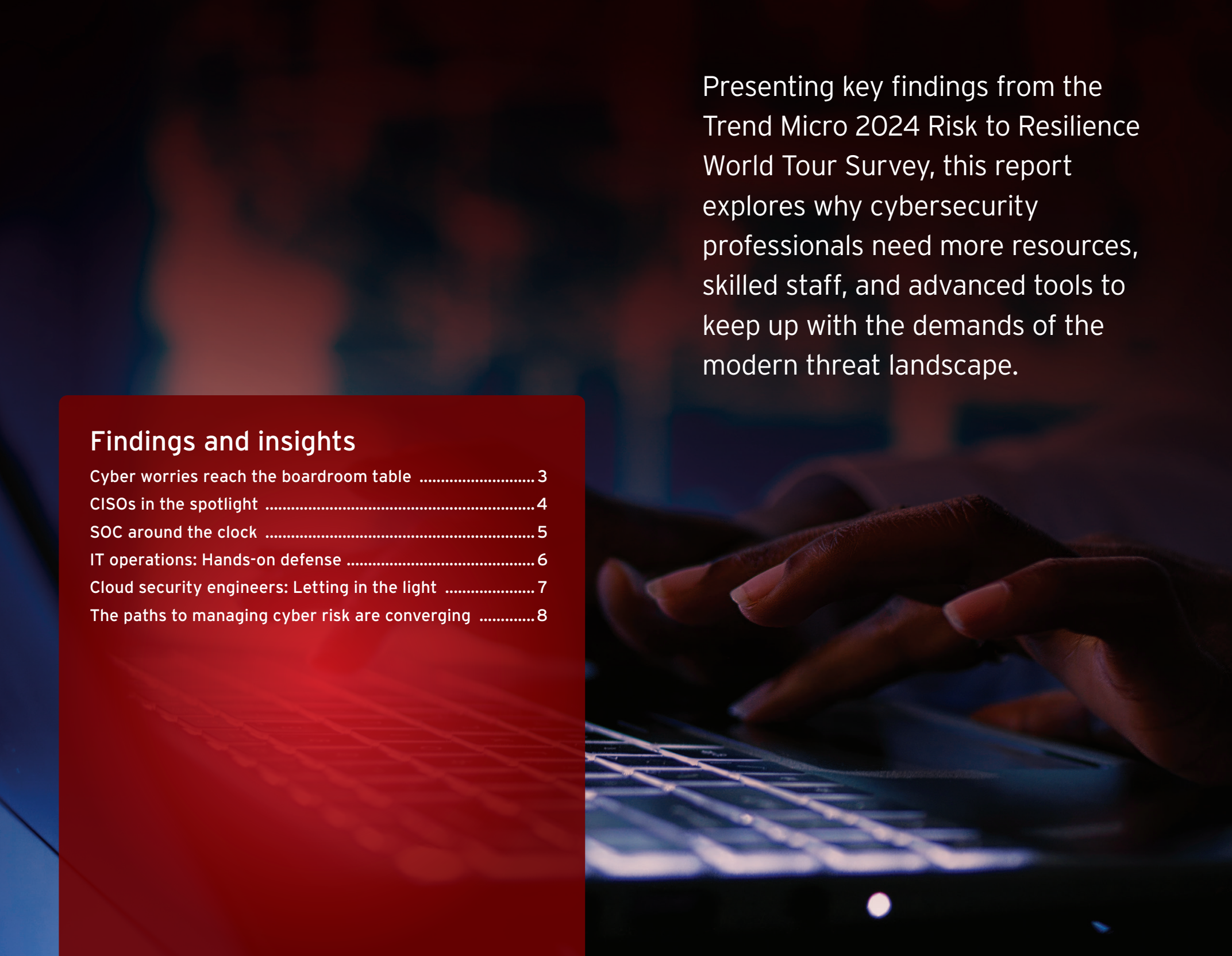
Findings from the Trend Micro 2024 Risk to Resilience World Tour Survey

September 2024

Presenting key findings from the Trend Micro 2024 Risk to Resilience World Tour Survey, this report explores why cybersecurity professionals need more resources, skilled staff, and advanced tools to keep up with the demands of the modern threat landscape.

Findings and insights

Cyber worries reach the boardroom table 3
CISOs in the spotlight 4
SOC around the clock 5
IT operations: Hands-on defense 6
Cloud security engineers: Letting in the light 7
The paths to managing cyber risk are converging 8



Cyber worries reach the boardroom table

Cybercriminals have more tools than ever to disrupt business operations, steal data for ransom, and manipulate employees into exposing sensitive information. Generative AI (GenAI) is taking those capabilities to new levels by enhancing phishing attacks and enabling audio and video deepfakes.

Security professionals are also facing new pressures from chief executives and corporate boards who increasingly understand the legal, financial, and reputational risks cyber threats pose to businesses.

To find out how these and other developments are shaping the day-to-day experience of cybersecurity professionals worldwide, Trend conducted its inaugural Risk to Resilience World Tour Survey. We surveyed more than 750 cybersecurity professionals in 49 countries, with a focus on four key roles:

- **Chief information security officer (CISO)**
- **Security operations center (SOC) team**
- **IT operations staff**
- **Cloud security engineers**

Highlighting key findings from the survey, this report explores why cybersecurity professionals need more resources, skilled staff, and advanced tools to keep up with the demands of the modern threat landscape. These individuals and teams see AI as both an adversary and a technology for good—and are keen to get out from under the clutter of point solutions by adopting platform methodologies.

AI and **zero-trust** architectures top the list of **technologies SOC teams want to explore** in the coming year to strengthen their security posture.

CISOs in the spotlight

The focus is on CISOs as cyber threats become increasingly prominent in corporate risk management discussions. Security leaders are expected to have the right answers regardless of whether the topic is AI, cloud, hybrid work, or any other facet of the IT environment—and they need more resources to meet this challenge.

Spending proves cybersecurity is a priority

Most CISOs (**61%**) say their budgets for 2024 were higher than in the previous year. This suggests the long-held view of cybersecurity as a cost center is giving way to recognition of its central importance to business operations.

Even so, **25%** of CISOs cite limited budget as a top challenge when it comes to retaining and hiring cybersecurity talent—second only to skills and knowledge shortages (**30%**). More money for hiring might help, but there's no guarantee that the required skills and knowledge are readily available. Instead, CISOs may be able to close gaps by integrating AI into their strategies, using it to lift the burden from their existing teams so they can do more—and even more efficiently.

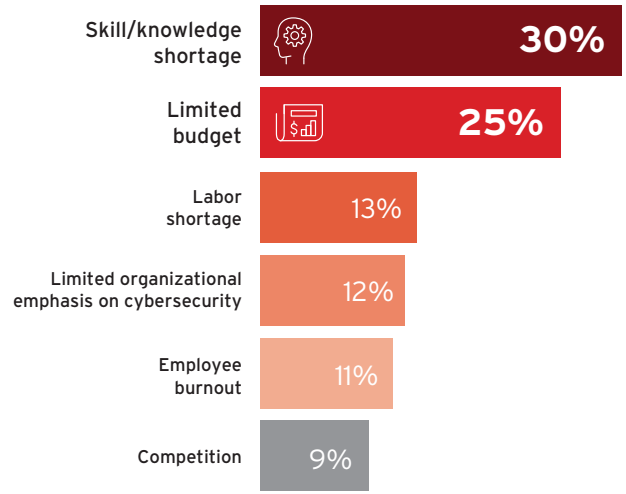
Not always on the same page

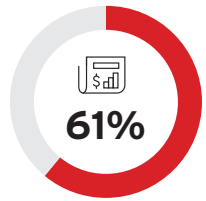
The general CISO consensus is that corporate directors have a decent understanding of cyber risks and challenges. On a scale of one to five, **89%** of CISOs rated their board's understanding at three or higher, with **24%** giving the board a five. When asked what aspects of communication with the board they find most challenging, their top answer (**23%**) was "communicating strategy or risk," followed by justifying spending on security tools and staffing (**17%**).

These findings suggest that, at the board level, understanding risks doesn't always translate into knowledge of how to mitigate them. In a separate global survey of 2,600 IT leaders, **80%** of respondents told Trend that their boards would only be spurred to act decisively on business risk if the organization suffered a major breach or financial loss. According to IBM's *Cost of a Data Breach Report 2024*, the average cost of such losses continues to climb—**up 10%** year over year by February 2024 to **US $4.88 million**—underscoring the importance of proactive risk management.

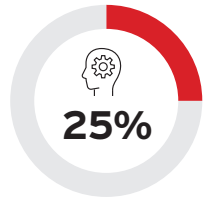
Ongoing engagement and correlated data will be the keys that enable CISOs to deliver crucial information to their boards. Unified platforms that consolidate telemetry, information, insights, and emerging technologies like next-generation security information and event management (NGSIEM) help to support both.

Top recruitment and retention challenges for CISOs





of CISOs say their budgets went up in 2024.



say they still need more to meet staffing needs.

SOC around the clock

SOC teams are on the front line of enterprise cybersecurity. Often stretched thin, overwhelmed with alerts, and on duty 24/7, they need integrated solutions to enable effective security operations and full attack surface management.

Too much information

SOC team respondents to the Risk to Resilience World Tour Survey echoed CISOs in citing insufficient team resources as a main challenge. **32%** put team size, resources, skills and training gaps at the top of their list. Alert volume and fatigue ranked second at **17%**. The two are arguably connected, as under-resourced teams have difficulty keeping up.

To find relief, SOC teams need to break down data silos, better prioritize threats and incidents, catch threats they're currently missing, and cut out the noise of false positives. Integrating toolsets and telemetry into a single platform with a unified view of the full environment is the goal, with AI-assisted correlation, triage, and analysis to automate and speed up time to action.

Looking to the next generation

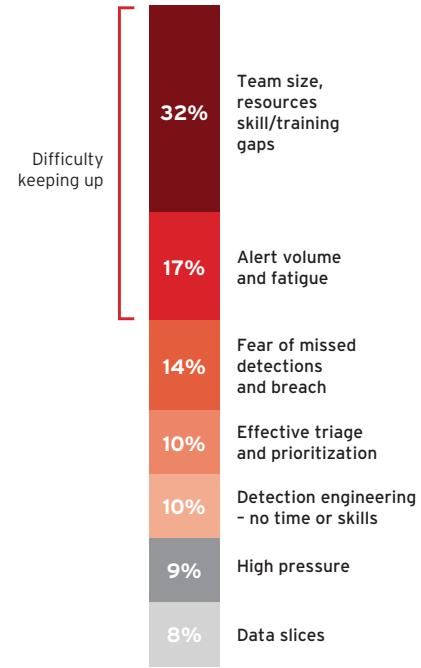
When asked what cybersecurity technologies they were most interested in exploring over the coming year, SOC respondents' top picks were AI and zero-trust architectures. Identity management rounded out the top three with privileged access and identity management (PAM and PIM) mentioned specifically.

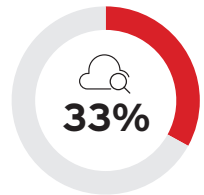
Endpoint detection and response (EDR) and network detection and response (NDR) can be combined via the native XDR or integrated next-generation security information and event management (NGSIEM) strategy to meet SOC needs. SOC teams can consolidate with the Trend Vision One™ platform to achieve the best possible integration and manageability.

Teaming up to mitigate risks

Because threats never sleep, SOC teams need to keep an eye on the enterprise environment 24/7. While **27%** do this with rotating schedules and another **25%** maintain on-call systems, the largest percentage of respondents (**33%**) rely on managed detection and response (MDR) or managed security service provider (MSSP) offerings. For small companies, MDR and MSSP services can fill critical capacity gaps. In larger organizations, they provide added expert support, follow-the-sun coverage, and peace of mind.

Top challenges for SOC teams





of SOC teams rely on MDR or MSSP services for 24/7 security monitoring.

IT operations: Hands-on defense

IT operations teams bridge the gap between operational continuity and resilient security postures by ensuring security protocols are applied. Those protocols include deploying security agents onto devices, correcting misconfigurations, and patching vulnerabilities. To be effective and timely, IT operations teams need seamless, continuous communication with their SOC peers.

Risk on the rise

The majority (**66%**) of IT operations survey respondents say their organization's risk level is increasing. Their ability to answer with confidence marks a shift even from five years ago, when teams had far less visibility into risk trends.

This sense of mounting risk may also be due to what IT operations teams cite as their topmost operational challenges: blind spots in the attack surface (**17%**) and the ability to prioritize remediations (**13%**). What goes unseen can't be mitigated, and ineffective prioritization may cause critical vulnerabilities to linger. Identifying risks up front to proactively reduce breach potential helps to prevent this.

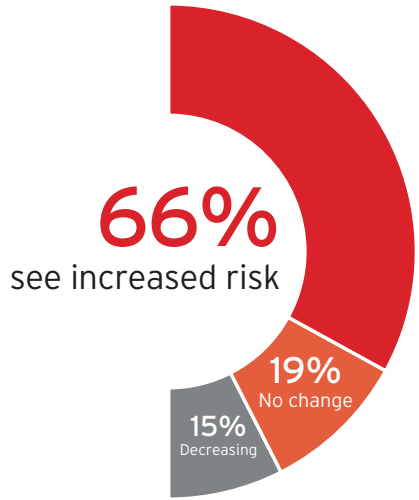
One particular risk on the minds of IT operations teams today is AI, primarily because they are involved directly in rolling out tools that use AI technology. Despite these continued and welcome innovations, corporate policies and user awareness of AI risks aren't often current with the fast-changing AI reality.

Security posture is an all-in endeavor

Although CISOs are responsible for overall cybersecurity efficacy and SOC teams help take critical protective—and proactive—actions, every part of the business has a role to play in establishing and maintaining a strong security posture.

To ensure they're working in complementary ways, IT operations require processes and regular cadence communication with the SOC. Platform-centric approaches support IT operations by integrating tools and telemetry while providing a foundation from streamlined communication, prioritization, and ticketing with other groups, including SOC and cloud teams.

IT operations see risk increasing



Blind spots in the attack surface are the **#1 challenge** for IT operations teams.

Cloud security engineers: Letting in the light

Modern enterprises depend on cloud services, applications, and infrastructure—making the protection of cloud assets and services vitally important. The expertise of cloud security engineers is required to provide visibility into the full range of cloud exposures.

Compliance is critical

While organizations can benefit immensely from the cloud, compliance needs to accounted for. Cloud environments require special protection because they typically store sensitive data that is governed by strong compliance requirements for data storage, protection, and transaction management. Customer data and personal identifying information (PII) breaches run the risk of negatively impacting your financial and/or reputational standing.

Gaining full visibility into cloud vulnerabilities, misconfigurations, and threat activity helps mitigate this risk. Yet cloud telemetry has long been siloed from the rest of the security stack. Cloud security engineers understand that this needs to change, with survey results indicating that mapping risk, misconfigurations and vulnerabilities is their top challenge (**27%**) when implementing and maintaining cloud security. Misconfigurations in particular continue to be the primary access point for attackers into cloud infrastructure.

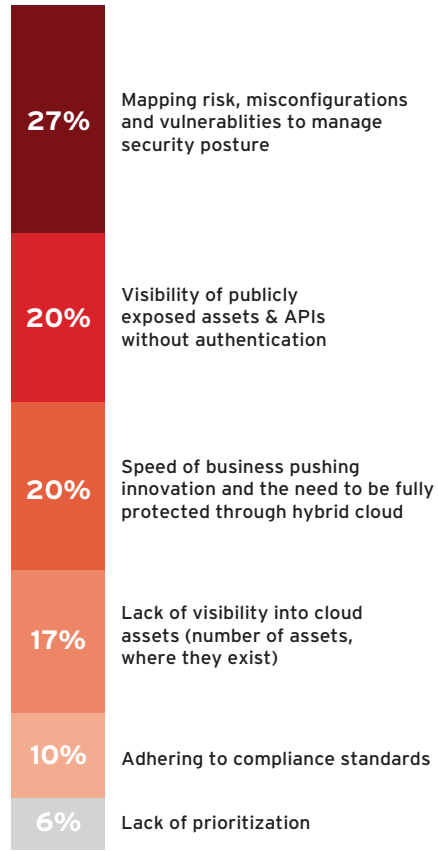
Minimizing exposure at high speed

The Risk to Resilience World Tour Survey indicates that cloud security engineers face other challenges as well. These include visibility of publicly exposed assets and APIs (**20%**) as well as, at the same percentage, businesses pursuing innovation while needing to fully protect data and applications in hybrid cloud environments.

What's needed most are tools to empower cloud security team analysts by enabling them to correlate data and automate responses across hybrid and multi-cloud environments. Operations then benefit from consolidation between cloud telemetry from the broader environment. This provides a single, streamlined view, integrating cloud risk with the rest of the IT environment.

Despite these risks and challenges, cloud security engineers are generally confident about their organizations' ability to mitigate cloud risk and maintain compliance. **92%** rate their confidence three or higher on a scale of five. A similar majority is confident in their ability to respond to cloud security threats, with **88%** rating theirs in this regard at three or higher and **25%** at five.

Cloud security engineers wrestle with risk



The paths to managing cyber risk are converging

CISOs and security teams battle with resource constraints. IT operations seek greater integration. Cloud security engineers strive for expanded visibility. All of these needs can be addressed with the AI-powered automation, contextualized data, and integration of a platform-based approach to cybersecurity.

Consolidating security within a single platform that can integrate third-party toolsets gives security leaders what they need with more flexibility, greater efficiency, minimized sprawl, and reduced total cost of ownership.

This approach meets security teams where they're at and respects the investments organizations have made to date, while transforming working models to drive strong user experience and security outcomes. Rich telemetry is more readily available, empowering teams to make more proactive and effective risk remediation decisions.

Trend Vision One delivers the benefits of a platform approach with comprehensive protection, prevention, detection, and response capabilities—all powered by AI and leading threat research and intelligence. It supports diverse hybrid IT environments, automates and orchestrates workflows, and delivers expert cybersecurity services to simplify and converge security operations holistically—all while measuring and communicating overall risk management and performance to stakeholders.

Explore more resources:

- **Watch the video** on Trend Vision One™ – Attack Surface Risk Management (ASRM)
- **Explore our Trend Vision One platform**

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend's AI-powered cybersecurity platform protects over 500,000 organizations and millions of individuals across clouds, networks, devices, and endpoints. Trend's platform delivers advanced threat defense techniques, extended detection and response (XDR), attack surface management (ASM), and integration across the IT ecosystem, including AWS, Microsoft, and Google. This enables organizations to better understand, communicate, and mitigate cyber risk. Trend's global threat research team delivers unparalleled intelligence and insights that power the platform and help protect organizations around the world from hundreds of millions of threats daily. With 7,000 employees across 70 countries, Trend is singularly focused on cybersecurity by enabling organizations to simplify their connected world. TrendMicro.com