TREND MICRO™

Trend Vision One™ - Threat Insights

See threats coming from miles away. Powered by Trend™ Research and global threat intelligence.

Another emerging threat is making the news, and you're scrambling to determine whether you're vulnerable. Don't wait to find out if you're next. Do you know who is targeting you? What vulnerabilities they are exploiting? How can you best protect your assets from specific threats? How can you defend your organization before the attackers even hit send on their phishing email?

Take back control of your environment with Trend Vision One – Threat Insights. Get the tools and confidence to hunt down threats and preempt alerts. Be better prepared for advanced, emerging threats that may be coming your way.

Empowering security operations

Threat intelligence curated by Trend Micro experts. As part of our Trend Vision One™ platform, Threat Insights provides you with rich context on latest vulnerabilities and IoCs, including emerging threats and threat actors that are already in or targeting your environment. This allows your SOC teams to elevate XDR alert investigations and ASRM vulnerability management.

Threat intelligence is woven into our DNA. With over 35 years of dedicated threat research, a global network of researchers and sensors, and the industry-leading Trend Micro™ Zero Day Initiative™–the number one bug bounty program–we offer unparalleled insight into emerging threats. Trusted by law enforcement, our unique perspective on cybersecurity threats remains unmatched.

Key capabilities

Customers like you utilizing XDR for endpoint, email, network, or cloud can enjoy these features without extra charge:

- **Endpoint, email, network, and cloud integration.** Threat intelligence sources allow you to expand beyond endpoints, across layers such as server, email, cloud, and network, providing you with a comprehensive and diverse depth of threat insights. Trend Vision One allows you to protect against alerts and threats derived from all security layers

- **Automated investigations.** Streamline threat identification and investigation by combining malware analysis, malware search, and threat insights. This integration enables you to reduce the time and skills required for manual incident investigations, allowing for quicker and more efficient threat response

- **Custom intelligence sweeping.** Automate the detection of threats within your environment by integrating custom, third-party intelligence feeds into your Trend Vision One platform. Receive tailored threat investigations to quickly identify and mitigate potential security risks

- **Open-source intelligence (OSINT) feeds.** Access collections of data gathered from publicly available sources to identify potential cybersecurity threats. These feeds enhance Trend Research, providing you with additional context and insights for improved threat detection and response

Key benefits:

- Stay ahead of latest threats
- Access in-depth indicators of compromise (IoCs) and vulnerability intelligence
- Streamline threat hunting
- Enrich XDR alert investigations
- Elevate attack surface risk management (ASRM) vulnerability management

"

The idea that I can bring IoCs very quickly and search across my organization is a game changer. I used to spend up to a week just to answer the question of "are we affected by this?"

"

Executive Director
Large University in USA

Key features

- **Emerging threats and threat actors.** Leverage proactive identification and analysis of new cyber threats and the entities behind them. This includes tracking and reporting on the latest cyber campaigns, converting findings into actionable intelligence, and monitoring command-and-control (C&C) servers to prevent ongoing breaches

  - Drill down to emerging threats and adversaries directly impacting your organization's industry and region
  - Discover who is exploiting vulnerabilities, their typical methods, their targets, and the most effective defense strategies against them
  - Understand the infection chain and map adversary tactics, techniques, and procedures to the MITRE ATT&CK Framework
  - Stay ahead of potential security risks and ensure timely response to evolving cyber threats

- **Vulnerability intelligence.** Gain a detailed analysis of known vulnerabilities, their exploitation, impacted assets, and mitigation strategies. By correlating vulnerabilities with emerging threats and actors, you have a comprehensive view of your security posture to take proactive measures and protect against both known and potential future threats

- **Enriched IoC intelligence.** Gain advanced, detailed information about specific indicators that may signify a cybersecurity threat. The search function enables your analysts to fully understand the impact and access richer context effortlessly

- **Threat hunting queries.** Proactively search for cyber threats within your environment. These queries, based on the latest intelligence, are tailored to detect and investigate suspicious activities or indicators of compromise. By utilizing these queries, you can uncover hidden threats and take swift action to mitigate potential risks

Threat intelligence is in our DNA

Extensive experience and coverage
Benefit from our vast library of insights drawn from 500,000+ commercial customers, millions of consumers, and a network of 250 million+ sensors spanning across 175+ countries. Leverage the broadest layers of native detection solutions for unparalleled diversity and depth of threat intelligence.

Global research network
Rely on our team of 400+ internal researchers worldwide for comprehensive regional threat analysis, crucial for safeguarding multinational operations.

Industry-leading intelligence
Curated threat data minimizes false positives, relieving your analysts of unnecessary workload burdens.

Critical source of vulnerability intelligence
By leveraging our ZDI program supported by 16,000 external researchers and events like Pwn2Own, customers gain access to a wealth of diverse threat intelligence.

Law enforcement collaboration
Trusted by global law enforcement, we actively collaborates on investigations to provide your team with critical insights.

Go deeper on XDR alerts and ASRM risks

Enrich XDR alert investigations
Leverage the effectiveness of the Trend Vision One XDR workbench alerts by providing comprehensive threat intelligence. This means going beyond just showing what happened and also revealing the "who, why, and how" behind the attack.
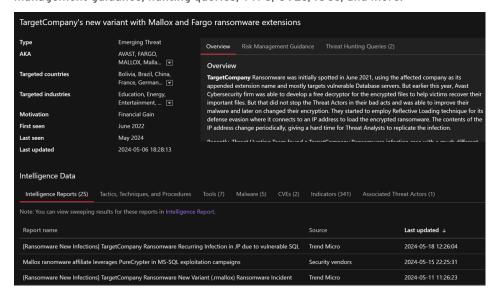
Elevate ASRM vulnerability management
Take your vulnerability management to the next level by showing emerging threats, threat actors, and hunting queries associated with the specific Common Vulnerabilities and Exposures (CVEs) in your environment. This allows your team to make faster and more informed risk management decisions.
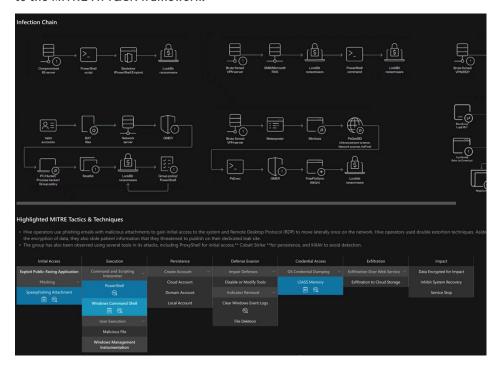
Features at a glance

	INCLUDED WITH XDR	TREND VISION ONE – THREAT INSIGHTS
Endpoint, Email, Network, Cloud Integration	●	●
Automated Investigations	●	●
Custom Intelligence Sweeping	●	●
Open-Source Intelligence Feeds	●	●
Emerging Threats and Threat Actors		●
Vulnerability Intelligence		●
Enriched IoCs Intelligence		●
Threat Hunting Queries		●

Rich details on a specific threat - targeted countries, industries, risk management guidance, hunting queries, TTPs, CVEs, IOCs, and more.
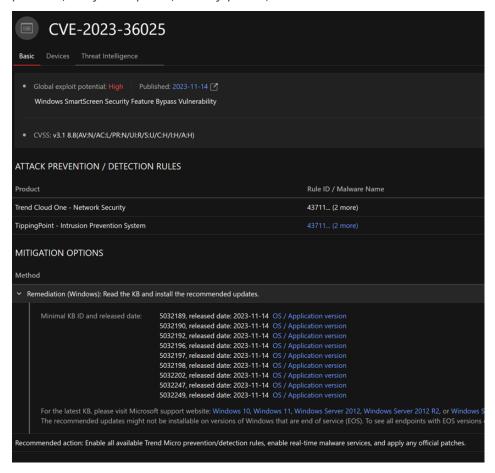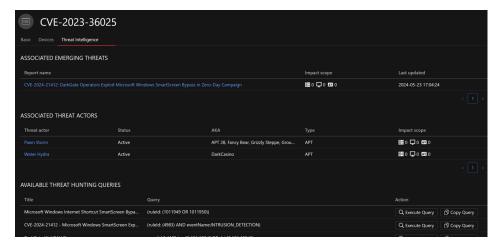

Mapped adversary tactics, techniques, and procedures to the MITRE ATT&CK framework.

Vulnerabilities intelligence allows a search for a specific CVE to get the exploit potential, mitigation options, hunting queries, and more.