TREND MICRO™

SOLUTION BRIEF

Trend Vision One™ AI Security

Stay aheadof emerging threats byproactivelystrengthening—and transforming—your security withourAI-poweredenterprise cybersecurity platform

AI for security teams

Imagine suffering an AI-related cyberattack, exposing sensitive data for days. According to the *World Economic Forum's Global Cybersecurity Outlook 2025* report, 66% of security professionals cite malicious AI as 2025's top threat. In other words, the time proactive AI security is now. That means staying ahead of adversaries and anticipating their next move.

Trend Vision One™ AI Security: Outsmart AI threats with smarter AI

Trend Cybertron, the industry's first proactive cybersecurity AI, is fully integrated within our Trend Vision One™ platform. It eliminates blind spots and vulnerabilities before attacks can occur, all while transforming your security operations with up to 99% faster remediation times per ESG's January 2024 report, *Analyzing the Economic Benefits of Trend Vision One*. Our AI Security solution integrates over 20 years of AI development and more than 35 years of threat intelligence, providing enterprise architects with the seamless integration, compliance, and scalability they need.

Trend Cybertron has agentic AI features that continuously evolve based on real-world intelligence and security operations, allowing it to adapt to emerging threats and provide increasingly efficient resolution strategies. Convert threat intelligence into actionable guidance, and empower your organization to shift from reactive to proactive security. Help your security operations team become more efficient while strengthening your security posture against today's most sophisticated cyber risks.

Trend Cybertron: AI powering proactive solutions

Trend Cybertron functions as a sophisticated "cyber brain" that analyzes data and telemetry to detect and correlate threats across your entire digital ecosystem. This integrated system identifies, predicts, and prevents threats. It also analyzes risk information to prioritize threats, predict attack paths, and provide actionable remediation guidance, all within a single interface.

KEY BENEFITS:

- Accelerate threat detection and response across your entire digital estate
- Reduce attack surface exposure by 94% through AI-driven path analysis
- Protect sensitive data and maintain regulatory compliance across borders
- Eliminate security blind spots before they can be exploited
- Defend against sophisticated AI-generated threats, including deepfakes and next-gen phishing

This advanced system reduces alert volume, uncovers previously unknown blind spots, safeguards sensitive data from potential exposure, and seamlessly links threat intelligence. Collectively, it delivers comprehensive protection that dramatically increases security operations efficiency beyond what traditional teams can achieve alone.

Inside Trend Cybertron

Trend Cybertron combines specialized cybersecurity large language models (LLM), datasets, machine learning technologies, natural language processing, and AI agents. It is trained by our global threat intelligence and vulnerability research, and it combines broad knowledge and expertise coverage across email, network, endpoint, identity, and cloud. This technology is designed for proactive prediction, prevention, detection, and response to risks and threats.

Trend Cybertron AI collection includes:

Specialized cybersecurity LLMs

- Purpose-built large language models specifically trained for security operations, threat detection, and risk management
- These models power Trend Companion™, our AI cybersecurity assistant that provides contextual guidance throughout the platform

Natural language processing (NLP):

- Anti-spam and invisible prompt injection prevention in email security
- Prompt injection prevention in network security
- Writing style analysis for business email compromise (BEC)
- Query generation assistance for security analysts

Machine learning (ML):

- Pre-execution and runtime ML for endpoint threat detection
- Computer vision algorithms for phishing detection and deepfake identification
- Alert prioritization to reduce noise and focus on critical threats
- Suspicious activity detection across the environment
- Network anomaly behavior detection
- Asset criticality calculation

Knowledge graph technology:

- Attack path prediction using knowledge graph inference
- Proactive threat hunting leveraging knowledge graph relationships
- Blast radius calculation to understand potential impact of security events

AI agents:

- Agentic AI that proactively identifies and predicts threats specific to each customer environment
- Continuous evolution based on real-world intelligence and security operations
- Adaptation to emerging threats with increasingly efficient resolution strategies

NVIDIA integration:

- Anomaly detection powered by NVIDIA Morpheus
- Identity security anomaly detection using NVIDIA Morpheus with AI detection mode
- Data classification with NVIDIA RAPIDS/CUDA, coming soon

Trend Companion:

- Context-aware cybersecurity assistant that helps with alert investigation
- Generates and suggests threat hunting queries
- Decodes and explains commands
- Explains events from observed attack techniques
- Generates case investigation reports and progress notes

These AI capabilities are fully integrated across the entire Trend Vision One platform, empowering your security teams with greater protection and operational efficiency across all security domains.

Trend Cybertron: AI Powering Trend Vision One Solutions

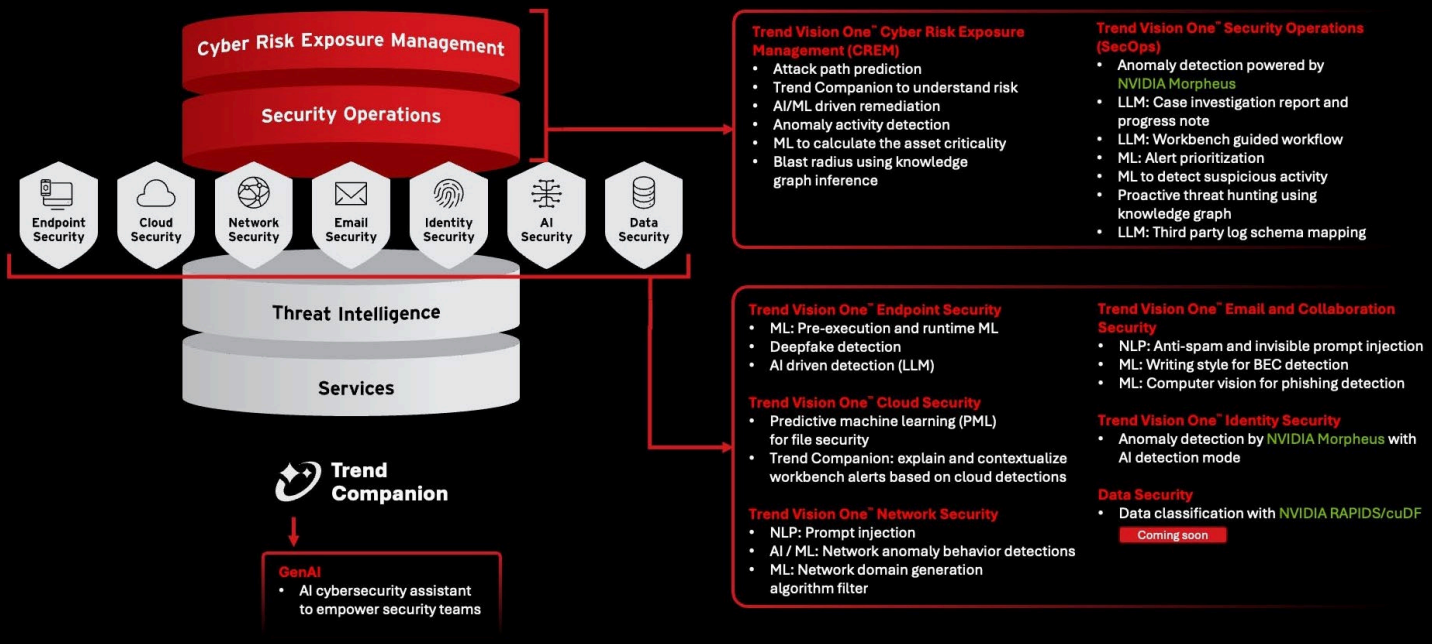

Figure 1: Trend Cybertron overview

Boost visibility, prioritize risks, and outpace adversaries with proactive solutions within Trend Vision One

Cyber Risk Exposure Management

- **Attack path prediction:** Harness a platform that automatically identifies potential attack vectors before they can be exploited, using knowledge graph technology to model relationships between assets and vulnerabilities
- **AI/ML-driven remediation:** Gain automatic recommendations and, in some cases, automatic implementation of remediation actions based on detected threats and vulnerabilities
- **Asset criticality calculation:** Calculate your asset criticality with powerful machine learning algorithms to help prioritize security resources

Security Operations automation

- **Automated alert prioritization:** Identify via ML algorithms which alerts require immediate attention, reducing alert fatigue by focusing your security teams on what matters most
- **Automated case reports:** Use LLM technology to generate investigation reports and progress notes, saving your analysts significant documentation time
- **Workbench guided workflow:** Leverage step-by-step automated assistance during threat investigation processes
- **Automated log schema mapping:** Enable automatic mapping of third-party log schemas with LLM technology, simplifying the integration of diverse data sources

Endpoint Security

- Leverage pre-execution and runtime ML models automatically detect and block malicious files and behavior
- Deepfake detection: A configurable security policy feature that employs advanced algorithms to analyze video calls in real time, identifying synthetic or AI-generated content

Cloud Security

- Gain automated contextualization of workbench alerts based on cloud detections
- Predictive machine learning (PML): Harness advanced machine learning technology using digital fingerprinting and API mapping, enabling your team to correlate threat information and perform in-depth file analyses to proactively detect unknown security risks

Network Security

- Access automated network anomaly behavior detection and domain generation algorithm filtering
- Utilize rules within Trend Vision One™ Zero Trust Secure Access (ZTSA) AI Service Access to protect against prompt injection, malicious LLM attacks, and data leakage through advanced content inspection and filtering for both public and private AI services

Email and Collaboration Security

- Implement NLP-powered anti-spam and phishing detection with automated invisible prompt injection prevention
- Utilize ML-powered business email compromise (BEC) detection that identifies compromised accounts and flags suspicious emails
- Access ML and computer vision to detect and block phishing attempts

Identity Security

- Implement automated anomaly detection for identity-based threats using NVIDIA Morpheus

Data Security

- Data security classification leverages NVIDIA RAPIDS/cuDF GPU acceleration to enable faster processing of large volumes of data, allowing for more efficient identification and protection of sensitive information through data loss prevention (DLP)

> The evolution of AI in the Trend platform is unique as it calculates our constantly changing risk profile and cross references millions of bits of data for custom threat intelligence. This cyber brain has made it possible to be more proactive than reactive with our entire security strategy.
>
> Stuart MacLellan
> CTO, NHS South London and Maudsley (NHS Foundation Trust)

TREND MICRO Vision One

AI-Powered Enterprise Cybersecurity Platform

Proactive security starts here

Trend Vision One is the only enterprise cybersecurity platform that centralizes cyber risk exposure management, security operations, and robust layered protection to help you predict and prevent threats, accelerating proactive security outcomes.

Sign up for a free 30-day trial

Learn more at eSecurity.com/contact/