TREND VISION ONE™

Security Operations (SecOps)

Detect, investigate, and respond proactively with XDR and Agentic SIEM and SOAR—leave attackers with no place to hide

In the race against threats, your security operations center (SOC) wins

Security teams carry the weight of protecting their organizations from threats no one else sees—often with too few people, limited budgets, and siloed tools. Burnout is common, and cross-team collaboration is more friction than function. Meanwhile, breaches are escalating. According to the Cost of a Data Breach Report 2024 by the Ponemon Institute and IBM, the average cost of a data breach hit $4.45 million in 2023—the highest ever recorded. There's no room for slow, siloed, or reactive security. Traditional security information and event management (SIEM) systems are expensive to operate, hard to scale, and overly reliant on manual tuning and investigation. Instead of accelerating response, they bury teams in complexity and noise.

SOC teams need more than just visibility—they need clarity, prioritization, and fast, coordinated action. Our Trend Vision One™ Security Operations (SecOps) solution brings together our award-winning XDR, Agentic SIEM, and Agentic security orchestration, automation, and response (SOAR) to help teams stay focused on what matters most. When threats move fast, your SOC team moves faster.

> **The Trend Vision One™ platform afforded us the opportunity to ingest all the information in one place and allowed our cybersecurity team to act on offenses and events across the board without the need to cross borders between the different IT organizations.**
>
> **Samer Mansour**
> Vice President, CISO
> Panasonic North America



Go beyond traditional reactive security with proactive capabilities

Built for the future

SecOps enables rapid setup and seamless integration, utilizing the most modern technology that delivers superior security capabilities at a lower cost, ensuring long-term scalability and efficiency from day one.

Large language model (LLM) advantage

Treat your schema like a language, using AI to understand the *intent* behind the data and reduce the need for manual rules.

Unmatched XDR foundation

Powered by our advanced native sensors, SecOps provides comprehensive visibility across all security layers. It fills critical detection gaps that traditional SIEMs leave exposed, ensuring better protection and fewer blind spots.

Effortless threat hunting

Our Trend Companion™ AI-powered cybersecurity advisor guides analysts through their investigations. It delivers AI-driven insights, automates routine tasks, and helps to reduce manual effort. This enables your SOC teams to focus on high-priority threats, accelerating response times and improving overall efficiency.

Understand your data. Act with intent.

The first Agentic SIEM that thinks in language, not just logs

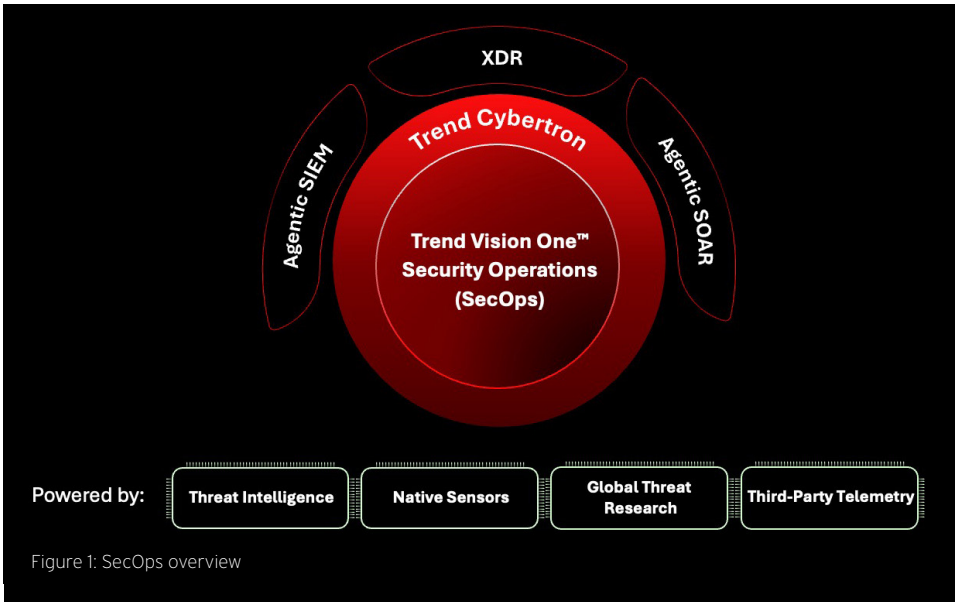


Figure 1: SecOps overview

Ingest third-party data seamlessly

Easily ingest both analytic data (for detection and hunting) and archival data (for compliance and long-term retention). Stay in sync with your evolving environment with real-time ingestion for any log type, at any scale.

Get actionable data observability

Turn diverse telemetry into meaningful insights with language-based correlation and AI-powered detections that cut through the noise. No manual efforts are required to parse data or create rules.

Streamline reporting and compliance

Make compliance effortless with built-in support for log retention, auditing, and regulatory reporting all in one console.

Simplify and scale data retention

Confidently meet compliance and retention needs with scalable, flexible strategies that preserve what matters without slowing down operations.

TREND Named a LEADER in 2024 Gartner Magic Quadrant for Endpoint Protection Platforms

FORRESTER WAVE LEADER 2024 Attack Surface Management Solutions

TREND Named a LEADER in 2024 Gartner Magic Quadrant for Email Security Platforms

2024 ENTERPRISE ATT&CK Evaluations

2024 MITRE ATT&CK™ Enterprise Security Evaluation results:

- 100% analytic coverage for all major steps (16/16)
- 100% analytic coverage in Linux and macOS for all sub-steps
- 100% analytic coverage in server platform (Windows/ Linux) for all sub-steps
- 99% analytic coverage for all sub-steps (79/80)

Implement powerful native threat coverage across every layer

- **Endpoint detection and response (EDR):** Detect and stop threats at the edge with deep endpoint visibility and real-time correlation
- **Network detection and response (NDR):** Expose hidden threats across unmanaged and rogue devices in your network
- **Cloud detection and response (CDR):** Secure workloads, containers, and clusters with full-stack cloud detection
- **Identity detection and response (ITDR):** Flag risky users and turn compromised identities into early threat signals
- **Email detection and response (EmDR):** Spot targeted attacks and account takeovers through behavioral email analysis
- **Data detection and response (DDR):** Track sensitive data movement and expose exfiltration attempts instantly.

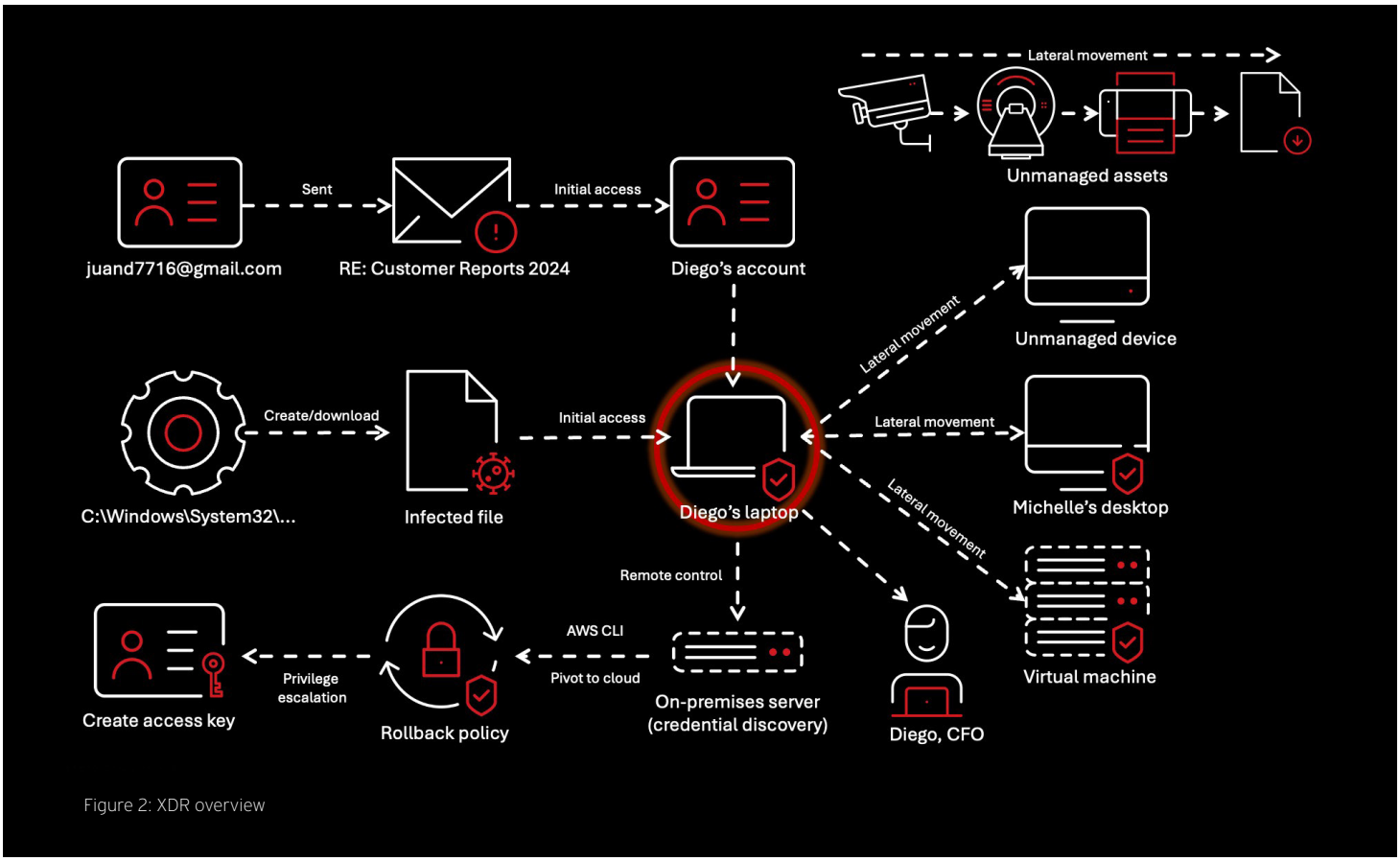


Figure 2: XDR overview

Redefining incident response with Agentic SOAR

Less noise. Faster action. Clearer value from every SOC move.

AI-powered investigations

Our workbench with auto-prioritization and AI summarizes incidents, guides next steps, and highlights what matters most so teams move from alert to action without guesswork.

End-to-end SOC automation

From triage to resolution, repetitive tasks are offloaded and optimized with AI and flexible case management. SOC teams stay focused on impact, not manual overhead.

Connected ecosystem

Our Agentic SOAR is built to connect, integrating into existing workflows and systems with open APIs, powering custom playbooks and real-time coordination.

Workflows that think ahead

Our Agentic SOAR equips analysts with intuitive, AI-assisted workflows to discover threats and discern context fast with fewer manual pivots.

TREND 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.

About Trend Micro

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, the Trend Vision One enterprise cybersecurity platform harnesses AI to protect hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. TrendMicro.com

Sign up for a free 30-day trial at TrendMicro.com/trial

Copyright ©2025 Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro logo, the t-ball logo, Trend Vision One, and Trend Companion are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. Trend Micro, the Trend Micro logo, and the t-ball logo Reg. U.S. Pat. & Tm. Off. [SB00_Security_Operations_Solution_Brief_250625US]

For details about what personal information we collect and why, please see our Privacy Notice on our website at: trendmicro.com/privacy