TrendAI™

Solution Brief

The Discovery Problem Is Solved. The Exposure Window Is the Crisis.

AI-powered tools have changed vulnerability research forever. The hard part is no longer finding flaws; it's closing the gap before an attacker walks through it.

Be ready for the frontier AI challenge

AI-powered tools can now surface critical exposures at a pace no human team can match. According to our **TrendAI™ State of AI Security Report**, 2,130 AI-related vulnerabilities were disclosed in 2025, a 34.6% increase year-over-year. By the end of 2026, that number is projected to reach 3,600, with nearly half rated high or critical severity.

Discovery isn't the real challenge. The bigger issue is what follows. Once a vulnerability becomes public, attackers can move quickly, sometimes within hours, while vendor patches often take weeks or months to arrive. It's within this window where most compromises happen.

Every major security vendor in this space scans, scores, and hands off to IT. None of them protect the gap before the patch exists. TrendAI™ does, by providing your teams with proactive protection that requires no system changes, pre-disclosure intelligence from the world's largest vulnerability research program, and risk prioritization grounded in your actual environment.

How TrendAI™ handles AI-powered discovery responsibly

TrendAI™ participates in Anthropic's Project Glasswing, an initiative focused on helping organizations identify and address vulnerabilities in critical software and infrastructure. Every AI-generated finding goes through human validation before it informs any protection or guidance delivered to customers.When a zero-day is found, our TrendAI™ Zero Day Initiative™ (ZDI) threat intelligence research team coordinates responsible disclosure with the vendor and deploys a virtual patch for customers often before the vulnerability is publicly known.

KEY BENEFITS

Close the exposure window

- Protect systems up to three months before vendor patches exist
- Block exploits at the network with no reboots or changes
- Cover legacy and OT systems that cannot be patched

Focus on what matters

- Prioritize based on real attack paths, not scores alone
- Correlate CVE data with your actual environment
- Reduce analyst triage time with automated workflows

Prove it to your board

- Rely on evidence-backed reporting from discovery through fix
- Get automated compliance mapping to NIST, FedRAMP, GDPR, and more
- Gain financial risk quantification for executive conversations

TrendAI™ ZDI and AI-powered research delivers the intelligence behind virtual patching

As monthly vulnerability disclosures reach record levels, the attack surface is not just growing; it's accelerating.

The volume extends far beyond any single vendor or disclosure cycle. TrendAI™ ZDI is the world's largest vendor-agnostic vulnerability research program, and the engine that powers virtual patching across our entire TrendAI Vision One™ industry-leading AI security platform. For more than 20 years, TrendAI™ ZDI has led global vulnerability disclosure, responsibly **surfacing 73% of all publicly disclosed vulnerabilities in 2024**, more than all other vendors combined, **according to Omdia**.

Where most security vendors respond to vulnerabilities after a public disclosure, TrendAI™ ZDI researchers discover and responsibly report zero-day vulnerabilities directly to affected vendors, creating a window of advance intelligence before other security organization can match.

TrendAI™ TippingPoint™ uses that intelligence to deliver network-layer protections up to three months before a vendor patch is publicly available. TrendAI Vision One™ Endpoint Security applies the same advantage to shield your devices and workloads up to 90 days ahead of official fixes. TrendAI Vision One™ Cyber Risk Exposure Management (CREM) then correlates active exploit targeting against your organization's specific asset inventory in real time.

With over 15,000 vulnerabilities disclosed since 2007 and 14 global threat research centers, TrendAI™ ZDI is the shared foundation that gives every layer of our virtual patching its lead-time advantage. For organizations that cannot afford to wait on vendor patch cycles, TrendAI™ ZDI is what makes the difference between being protected and being exposed.

Three capabilities that work as one

Most security programs treat discovery, protection, and remediation as separate problems. TrendAI™ connects all three, so a vulnerability found by our research team becomes a network-level block within hours and eventually a prioritized, evidence-backed remediation your board can see.

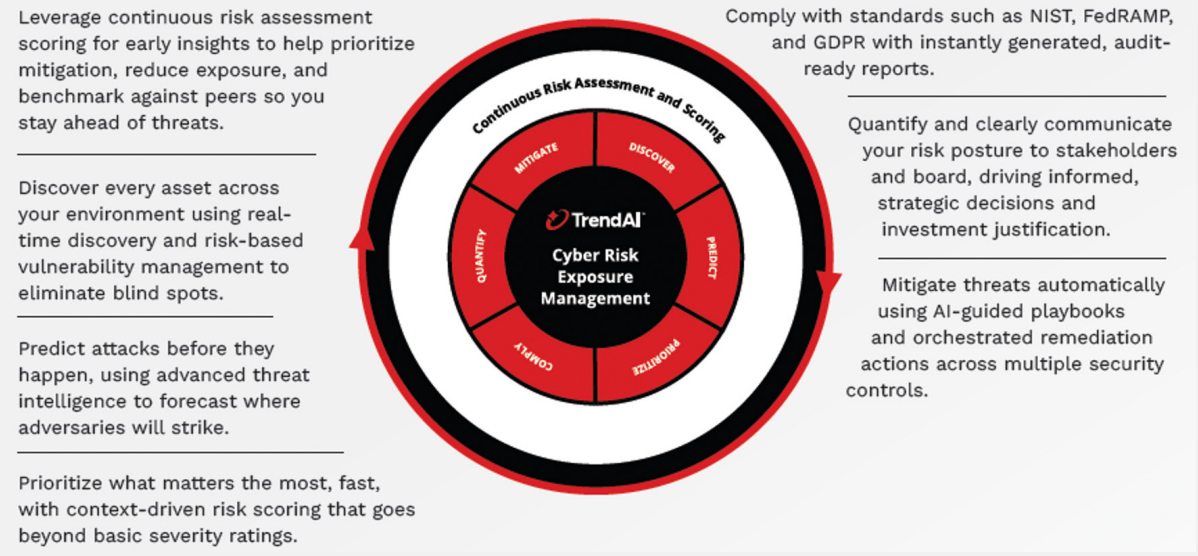
Know where you're exposed before attackers do with Cyber Risk Exposure Management

The attack surface is not just growing, it is accelerating. As your organization manages thousands of assets across on-premises, cloud, and hybrid environments, the volume of exposures your security teams must assess and act on is growing faster than any manual process can handle. These exposures span vulnerabilities, misconfigurations, identity risks, unsanctioned AI tools, and exposed APIs. CREM connects attack surface discovery, risk prioritization, and protection coverage into a single continuous workflow, giving your security team a clear, risk-ranked view of where your greatest exposures are before attackers can act on them. Close that gap by continuously discovering every asset across your environment, scoring risk in real time across the full exposure surface, and correlating that data with active threat intelligence from TrendAI™ ZDI. Surface which exposures are being actively targeted right now, and act before attackers do. Shift your team from reacting to alerts to making deliberate, risk-informed decisions. Ensure your security investments are directed at the exposures and assets that represent the highest real-world risk to your business.

INDUSTRY RECOGNITION

IDC MarketScape Leader	The Forrester Wave™ Leader	The Forrester Wave™ Leader	Gartner Magic Quadrant Leader	Omdia Research Leader
Worldwide Exposure Management, 2025	Network Analysis and Visibility Solutions, Q4 2025	Attack Surface Management Solutions, Q3 2024	Endpoint Protection, 21 years running	Global vulnerability research and disclosure since 2007

Ensure your security teams have a holistic approach to cyber risk and exposure management.



From vulnerability discovery to protection in three days

TrendAI™ ZDI and AESIR, our AI-powered security research offering, work together through an automated pipeline to accelerate virtual patch delivery to as fast as three days from vulnerability discovery to protection. AI-assisted triage accelerates protection rule development, with human experts serving as the final gatekeeper for review, testing, and validation. The result is a streamlined delivery process that ensures your organization is protected before attackers have time to weaponize a vulnerability.

TrendAI™ TippingPoint™ Intrusion Prevention System (IPS) virtual patching stops exploits before a patch exists

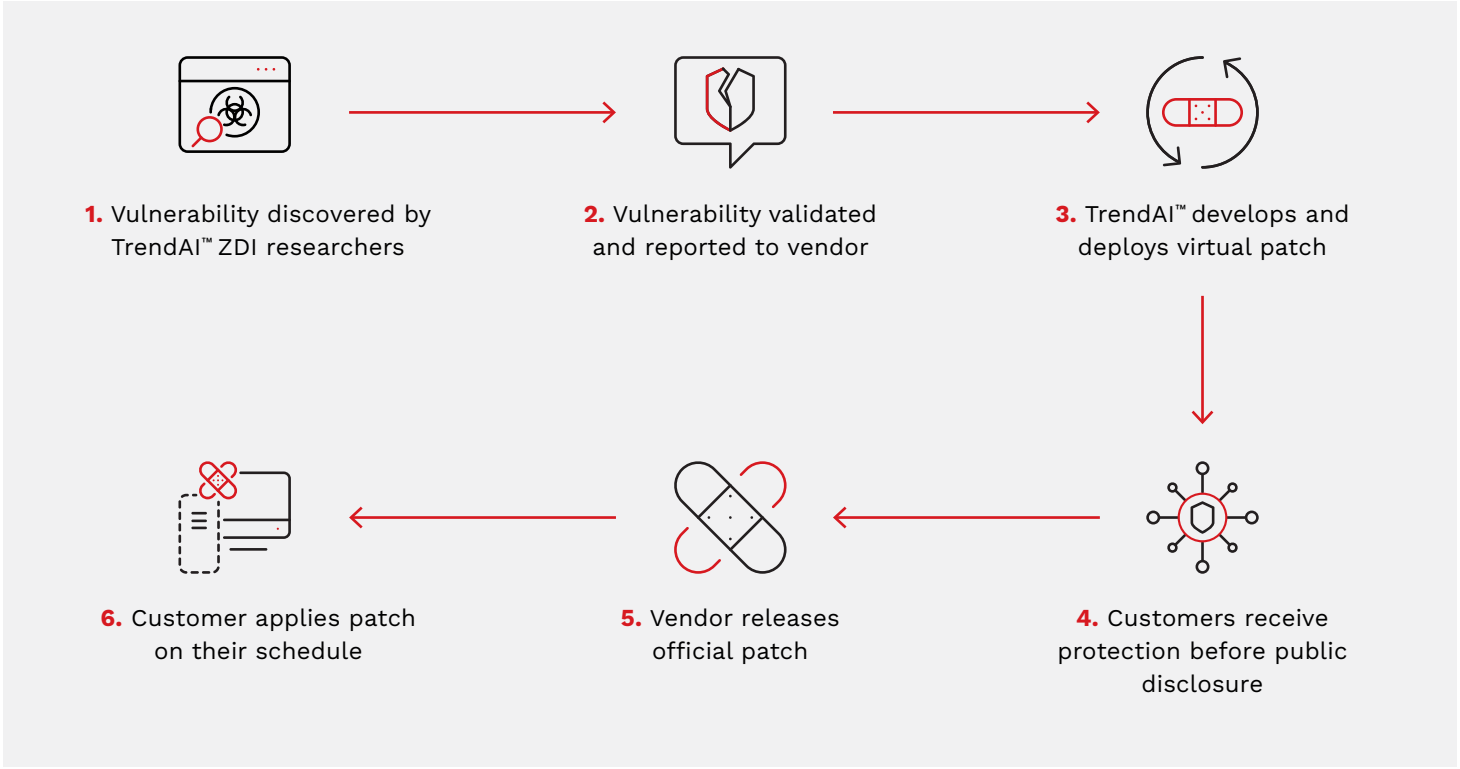
IPS virtual patching gives you immediate protection against network vulnerabilities. Prevent exploit attempts at the network layer without having to immediately apply a software patch or disrupt critical operations. As vulnerabilities continue to be discovered at an accelerating pace, many organizations face a growing gap between when a vulnerability is identified and when a permanent patch can be tested, approved, and deployed. IPS helps you close this exposure window by leveraging industry-leading threat intelligence and TrendAI™ ZDI research. Benefit from protections that block malicious attempts targeting your vulnerable systems up to three months before a vendor patch is publicly available.

This is especially valuable for mission-critical environments such as industrial, manufacturing, energy, and legacy IT systems, where uptime requirements, operational constraints, or unsupported technology can make traditional patching difficult. By extending your organization's ability to safely manage patch cycles, IPS enables your security teams to reduce cyber risk while maintaining operational continuity.

Protect every asset, wherever it lives, with endpoint virtual patching

TrendAI Vision One™ Endpoint Security delivers virtual patching at the system level, allowing you to protect servers, workloads, and endpoints directly from vulnerability exploits without waiting for a patch to be approved and deployed. While TippingPoint secures the network perimeter, endpoint virtual patching lets you follow the asset wherever it resides, whether it's on-premises, in the cloud, or across distributed environments. This is critical for organizations running workloads that cannot be immediately patched due to application dependencies, change control windows, or vendor support constraints. Powered by TrendAI™ ZDI research, endpoint virtual patching gives you host-level protection up to three months before official patches are available, including coverage for legacy and end-of-support operating systems. Together with TippingPoint and CREM, you gain complete layered coverage. Gain the intelligence to know what's at risk, the network protection to stop exploits at the edge, and the host-level defense to protect every asset that sits behind it.

How it works:



1. Vulnerability discovered. A security flaw is identified in software through researchers, TrendAI™ ZDI, or third-party disclosure. No fix exists yet, and the attack surface is open.

2. Vulnerability validated. The flaw is confirmed, severity is assessed, and the vendor is notified. The window of exposure begins.

3. Develop virtual patch. Before any official fix exists, TrendAI™ develops a detection and prevention rule that blocks any exploit attempt targeting that vulnerability. No code change required.

4. Customer receives protection. The virtual patch is delivered automatically. Customers are shielded from exploitation even though the underlying vulnerability still exists in their environment.

5. Official patch released. The software vendor publishes an official code-level fix, often weeks to months after TrendAI™ customers were already protected.

6. Customer applies patch. The organization deploys the vendor patch through its standard change management process. TrendAI™ continues to act as a safety net for any systems still pending remediation.

Built for industries where downtime is not an option

Every organization faces environments where taking a system offline for patching is not always a practical option, and where a breach can mean operational disruption, financial loss, or regulatory consequence. Whether the pressure comes from compliance requirements, the speed at which attackers move after a disclosure, or the operational cost of unplanned downtime, the gap between exposure discovery and remediation cannot be left unmanaged. TrendAI Vision One™ allows you to close that gap with inline protection, pre-disclosure intelligence, and evidence-backed remediation so critical operations stay running, and your security teams stay ahead.

New. Anthropic Claude compliance API integration

TrendAI™ has integrated the Claude Compliance API into TrendAI Vision One™, giving your security, IT, and compliance teams centralized visibility into Claude usage across your organization. This connects Claude data to the telemetry from the rest of your attack surface, so your AI activity doesn't exist in a silo. Organizations running Anthropic Claude Enterprise or the Anthropic Claude API can now bring that activity into the security workflows they already have in place. Two purpose-built collection methods support different monitoring and data residency requirements. AI is no longer a blind spot, it's part of your unified security picture.

Detect sensitive data exposure

Identify when PII, PHI, credentials, source code, or confidential documents are shared with Claude and surface which users and projects carry the highest risk.

Surface policy violations and prompt attacks

Detect prompt injection attempts, jailbreak patterns, and harmful content in conversations before they become incidents.

Connect AI activity to your full attack surface

Via TrendAI™ Agentic SIEM, Claude logs correlate with signals from endpoint, identity, network, cloud, and email, so you can identify insider risk and anomalous behavior across your whole environment.

Build a defensible compliance record

Every AI interaction is logged, auditable, and available for compliance and governance reporting, so you can give boards and regulators evidence of responsible AI adoption.

TWO DISCOVERY PATHS, ONE ADVANTAGE

Not all vulnerabilities are discovered the same way. Anthropic Claude Mythos uses AI-driven code and exploit analysis to surface exposures at machine speed, scanning codebases and identifying weaknesses faster than any human team can. TrendAI™ ZDI brings a mature vulnerability intelligence program built on expert research, independent researcher submissions, Pwn2Own™ competition findings, coordinated disclosure, and AI-assisted analysis accumulated over more than 20 years.

These two capabilities do not overlap. They work together. Mythos accelerates discovery at scale. TrendAI™ ZDI delivers depth, context, and advanced intelligence across discovery paths that automated analysis alone cannot reach. Together, they give your organization broader coverage and earlier warning across a threat landscape that is growing faster than any single approach can keep pace with.

Stay ahead of the exposure window

AI is accelerating vulnerability discovery at a pace that has fundamentally outrun traditional security approaches. What once took researchers weeks now takes hours, and the vulnerabilities being found are increasingly critical. For your organization, this means the window between discovery and exploitation is shrinking while the volume of exposures keeps growing.

TrendAI Vision One™ is built for this reality. By combining pre-disclosure intelligence from the TrendAI™ ZDI, virtual patching that protects systems before a vendor patch exists, and risk-based exposure management that cuts through the noise, your organization turns AI-accelerated discovery into protection, rather than compounding risk.

The organizations that stay ahead will not be the ones that patched fastest. They will be the ones who closed the exposure window before attackers could use it.

About TrendAI™

TrendAI™, a business unit of Trend Micro and global AI security leader, empowers enterprises, governments, and organizations with proactive solutions designed to inspire innovation and eliminate risk. Taking the uncertainty out of security, TrendAI™ protects over 25,000 enterprise organizations and millions of individuals across AI, cloud, networks, endpoints, and devices.
AI Fearlessly. **trendaisecurity.com**

Sign up for a free 30-day trial

Learn more at **trendaisecurity.com**