Emerging Tech: Harnessing Domain-Specific Language Models for Enhanced Preemptive Cybersecurity Strategies

3 December 2025 - ID G00836934 - 10 min read

By: Esha Bhatia, Srushti Bhakta

Initiatives:Craft World-Class Product Strategies; Emerging Technologies and Trends Impact on Products and Services

> Security product leaders must adopt domain-specific language models to stay competitive in the AI race. This research guides you on integrating these tools for proactive and preemptive cybersecurity strategies.

Overview

Key Findings

- Adopting DSLM-powered security capabilities is no longer optional for security product leaders — it is a strategic necessity. Integrating these capabilities beyond traditional applications will drive competitive differentiation and future-proof against AI-driven threats
- Product leaders who apply domain-specific language models to proactive and preemptive capabilities stand to gain market leadership and create material differentiation.

Recommendations

- Conduct a comprehensive workflow assessment by collaborating with GRC, IAM, and IT operations teams to map current fragmented processes and identify repetitive, high-volume tasks for DSLM-driven automation.
- Prioritize preemptive security by developing “left-of-boom” capabilities, such as implementing agentic threat hunting and adversarial simulation, to actively and dynamically deny attack vectors before they can be exploited.

Analysis

Technology Description

The traditional reactive security model is increasingly insufficient against rapidly evolving, AI-accelerated cyberthreats, posing significant enterprise challenges. Threat actors leverage advanced AI, make it difficult for human-centric reactive defense to properly mitigate threats. This necessitates a fundamental shift toward proactive and preemptive cybersecurity capabilities that actively deceive, deny, or disrupt threats before they can impact an organization (see Tech FutureSight: Preemptive Cybersecurity Is the Only Way to Secure Emerging AI Attack Surfaces).

DSLMs are central to this transformation, enabling security operations to “shift left “ of traditional incident response by:

- Predicting issues
- Simulating attacks
- Countering sophisticated patterns in real time

DSLMs trained explicitly on cybersecurity datasets like CVE (common vulnerabilities and exposures) reports, threat intelligence feeds, and SOC (security operation center) playbooks, ensure:

- Specialized vocabulary
- Deep contextual understanding
- Higher accuracy than general-purpose large language models (LLMs)

Proactive cybersecurity encompasses all measures taken to anticipate threats and improve an organization’s overall security posture before an attack fully materializes or causes significant harm. While supporting preemptive actions, proactive measures focus more on anticipation, preparation, and continuous improvement of defenses rather than direct, real-time intervention with an adversary. Examples of proactive cybersecurity, often powered by DSLMs:

- **Detection engineering and tuning:** Continuously evaluating and auto-tuning detection rules to maintain best-in-class coverage against evolving threats and detection coverage gaps

- **Risk identification and assessment:** Proactively identifying user-related risks by comparing real-time behavior to historical patterns and augmenting existing security controls

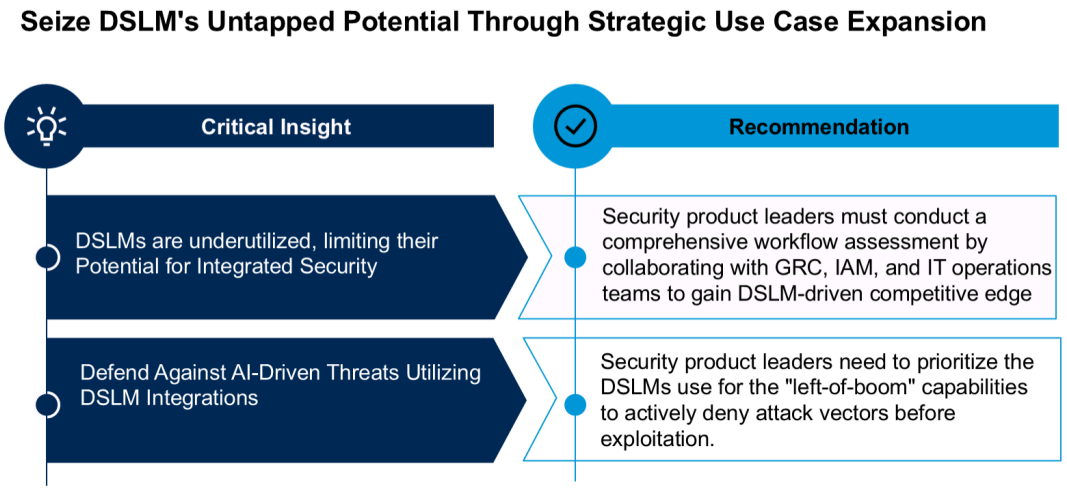
Preemptive cybersecurity is characterized by an approach to prevent or deter cyberattacks from achieving their objectives. Use cases where DSLMs can operationalize preemptive defense:

- **Deceive:** DSLMs can generate dynamic deception environments at scale, compelling adversaries to reveal their tools and tactics while creating a high-fidelity data stream to train and improve defensive AI continuously.
- **Deny:** By applying deep semantic understanding to vast streams of threat intelligence and real-time network behavior, DSLMs can predict likely attack paths and automate the hardening of the attack surface, denying adversaries their targets.
- **Disrupt:** Acting as an intelligent orchestration engine, DSLMs can trigger high-speed, automated responses to the earliest indicators of an attack, disrupting the cyber kill chain before an adversary can achieve their objectives.

Adopting DSLM-powered proactive and preemptive security capabilities is no longer optional for product leaders — it is a strategic necessity. Integrating these capabilities will drive competitive differentiation and future-proof against AI-driven threats.

Figure 1 outlines critical insights and actionable recommendations for expanding the use cases of DSLMs in proactive and preemptive security capabilities.

Figure 1: Seize DSLMs' Untapped Potential Through Strategic Use-Case Expansion



Source: Gartner
820992

Gartner

Critical Insight: DSLMs Are Underutilized, Limiting Their Potential for Integrated Security

Near-Term Implications for Product Leaders

Providers are now strategically expanding DSLM use cases beyond traditional applications to unlock their full potential and gain a competitive edge. When DSLMs are deployed reactively and within silos, their potential to create a cohesive and powerful security posture for the entire enterprise remains largely untapped. Without a unified approach, achieving an integrated defense will take much longer. Individual tools and DSLM-powered agents will struggle to communicate and collaborate effectively. This fragmented strategy means that while some individual tasks may see efficiency gains, the overall security posture will remain suboptimal, unable to adapt to the accelerating pace of AI-powered adversarial tactics.

Limiting DSLMs to reactive alert handling misses the more impactful opportunities to automate proactive security measures, streamline GRC processes, or enhance exposure management. This limited scope restricts potential cost savings and efficiency gains and hinders the ability to unify disparate security tools and create a truly integrated security posture across the enterprise.

Providers are pivoting their strategies to emphasize the holistic and proactive value of DSLMs to bridge organizational silos, moving beyond reactive point solutions to address an enterprise's integrated security posture. There is a clear ambition among vendors to leverage DSLMs for more holistic and cross-functional automation across the enterprise:

Recommended Actions for the Next Six to 18 Months

- Conduct a comprehensive workflow assessment by collaborating with GRC, IAM, and IT operations teams to map current manual processes and identify repetitive, high-volume tasks ripe for DSLM-driven automation.
- Establish a shared AI-driven vision by engaging multiple stakeholders across security, IT, data, and compliance to foster cross-functional alignment for broader DSLM implementation and value demonstration across silos.

Critical Insight Analysis

The confinement of DSLMs to existing, often reactive, security silos overlooks the substantial efficiency gains possible from their strategic application in areas like:

- Automated audit tasks
- Unified SaaS permissions
- Proactive vulnerability prioritization

By bridging these silos, DSLMs can transform security into a strategic enabler for the entire enterprise.

According to our mini case-based research study with 16 vendors, 60% of the vendors emphasized the broader applicability of DSLMs.

Airrived explicitly positions itself as an enterprise agentic AI platform that enables organizations to evolve from a single agent to an interconnected network of agents powering multiple teams. It supports agentic automation across SOC, audit, IAM, vulnerability, risk, and business ops and aims for cross-functional agents spanning SecOps, ITOps, and DevSecOps to bridge silos. Airrived also stated its expansion into networking and IT, automating anomaly detection and root cause analysis for engineers, and streamlining audit tasks.

Cisco develops solutions for both AI-driven security and security-driven AI. The Cisco Foundation AI organization is focused on creating transformational AI technology for cybersecurity applications, including the development of domain-specific security models for tasks such as attack simulation and vulnerability prioritization. Companies will be able to embed security reasoning for infrastructure-as-code and CI/CD pipelines. Separately, Cisco also protects first-party AI applications with its AI Defense product, which uses detection models in algorithmic red teaming and guardrails for runtime protection.

Conifers plans to expand its use cases to broader security domains such as cloud coverage, data loss prevention (DLP), cloud security posture management (CSPM), and reconnaissance, with industry-specific scenarios across IT and OT environments. They are actively building toward security-specific artificial general intelligence (security-AGI).

CrowdStrike envisions DSLMs supporting adjacent use cases such as IT, fraud, DevOps, compliance, geopolitical risk, and risks to physical safety, and it plans to develop agents for all paramount security and IT roles. They see extreme opportunities to co-develop new capabilities across security, IT, and risk functions.

NSFOCUS utilizes SecLLM NSFGPT (Chinese name Fengyunwei) to build an AI agent that focuses on solving various security tasks in the field of security, including threat failure and risk analysis, automated threat response, threat tracing analysis, intelligent penetration testing, attack disposal, security assessment, and more. It will establish an AI security base platform to empower relevant security product solutions, launch multidimensional agents to penetrate various business scenarios, improve efficiency and accuracy, reduce the impact of risks, and protect customer asset security. They will expand agents into code audit, vulnerability mining, and asset mapping to enrich risk mining capabilities. Currently, there are 20+ domain-specific agents in security operations.

Red Canary plans to expand its security data lake to ingest data from business applications (such as Salesforce or SAP), physical security systems, and even code repositories, providing a holistic view of an organization's risk.

Critical Insight: Defend Against AI-Driven Threats Utilizing DSLM Integrations

Near-Term Implications for Product Leaders

Product leaders are accelerating DSLM integration for proactive security use cases like automated AI red/purple teaming, predictive vulnerability prioritization, and AI-driven deception. To drive adoption and ensure resilience against evolving threats, they're implementing trust gates via explainability, data privacy, and human-in-the-loop validation.

Providers are embedding DSLMs as modular components, core AI agents, or orchestration engines to enable early threat detection, predictive analysis, and automated mitigation across multistep security workflows.

Recommended Actions for the Next Six to 18 Months

- **Proactively detect, simulate, and counter sophisticated attack patterns in real time,** by integrating DSLM-based agentic threat hunting and adversarial simulation tools into platforms shifting security "further to the left."
- **Prioritize solutions that deny attack vectors** by focusing on use cases such as DSLM-powered cloud misconfiguration remediation and autonomous email security agents, among others, which uncover and neutralize threats before manual intervention.

Critical Insight Analysis

The rise of AI-powered threats is driving a shift from reactive to proactive cybersecurity. Traditional models can't keep pace, so defenders are shifting "left" to neutralize threats before they have an impact. Powered by DSLMs, this evolution enables autonomous agents to detect, deter, and respond early — transitioning from a human-in-the-loop to a human-on-the-loop approach with transparent oversight (see Tech FutureSight: Preemptive Cybersecurity Is the Only Way to Secure Emerging AI Attack Surfaces).

Accenture is leveraging cyber deception tactics — like fake credentials, misinformation on the darknet, soft target bots, and spoofed Shodan data — to manipulate threat actors' behavior. This proactive strategy shifts control to defenders, disrupting adversaries and forcing them to scale their efforts.

Airrived uses autonomous agents for real-time threat hunting and adversarial simulation. Their DSLM-powered tools autoremediate cloud misconfigurations and detect advanced phishing, neutralizing threats across multicloud and email environments.

AiStrike uses DSLMs for proactive threat intelligence, building a real-time encyclopedia of emerging threats and autogenerating SIEM rules. Their roadmap includes automated exposure management and SIEM-less detection for direct threat hunting on customer data lakes.

Cisco AI Defense is designed to "detect and block malicious AI requests at the point-of-presence" before they reach a customer's environment, thereby denying the threat. Their foundation AI product focuses on proactive defense, including attack simulation and vulnerability prioritization. Plans include enhancing proactive threat detection using continuous AI threat intelligence to anticipate new attack vectors and advancing automated AI model validation and runtime protection to identify vulnerabilities.

Deloitte's ARTIC functions as a structured reasoning engine over curated threat intelligence, feeding insights into proactive engagements. **Deloitte's Agent Smith** is designed for offensive security teams, supporting Penetration Test, Red Team, Breach Attack Simulation, Social Engineering, and Purple Team support, which involve simulating attacks to gather intelligence on adversary tactics and improve defenses. **Deloitte's next-generation Active Cyber Defense (ACD)** provides autonomous cyber defense recommendations and responses through an AI agentic recommender system. It focuses on proactive threat mitigation by integrating automated defense deployment with data lake infrastructure to recommend and implement defensive actions based on near real-time analysis.

IBM plans to include risk profiling, AI threat imputation, predictive threat intelligence, predictive threat detection, and autonomous policy authoring management as future use cases, which are proactive measures designed to identify and address threats before they fully materialize.

Imperum offers powerful utilities such as a Threat Intel Fetcher that retrieves the latest CVE list from the National Vulnerability Database (NVD), filters by critical severity, and outputs vulnerable CVEs — proactively informing defenses against known threats. Combined with Imperum's native Forensics and Investigation Agent, organizations can automatically trigger playbooks to block or uninstall any vulnerable application until it is patched. This end-to-end capability delivers a comprehensive approach to managing the entire vulnerability life cycle.

Red Canary uses user behavior baselining to detect risks and is advancing toward predictive threat intelligence to spot emerging attack patterns early. Their automated posture management continuously identifies and remediates misconfigurations, vulnerabilities, and policy violations — acting as a proactive risk reduction engine.

Acronym Key and Glossary Terms

IAM	Identity and access management
GRC	Governance, risk, and compliance
CI/CD	Continuous integration/continuous delivery

Evidence

This document is part of Gartner's mini case-based research (CBR) into the current state and future direction of domain-specific language model capabilities in security operations. During a three-month research effort that commenced in June 2025, Gartner analysts conducted surveys and interviews with 16 global security vendors.

Gartner analysts engaged vendors in two primary discussions:

- A vendor briefing to understand product capabilities, features and related go-to-market strategies
- A vendor interview reviewing verifiable real-world use cases demonstrating the adoption of the vendor's innovation, where the customer achieved desired outcomes

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Quick Answer: How Will Domain-Specific Language Models Shape the Future of Security Operations?

Emerging Tech: AI Vendor Race: Lead With DSLMs or Lag Behind in Cybersecurity Autonomy

Emerging Tech: AI Vendor Race: Pivot to Preemptive Exposure Management Services to Grow Revenue