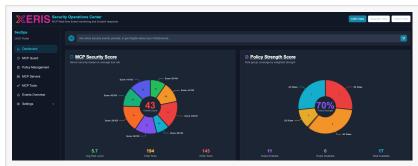# Xeris Announces the First MCP-XDR (Extended Detection and Response) System Powered by Patent Pending Technology

TEL AVIV, ISRAEL, June 20, 2025 /EINPresswire.com/ -- Xeris is proud to announce the launch of the industry's first MCP-XDR (Extended Detection and Response) system, built on patent pending technology and designed to meet the security demands of enterprise AI deployments. This breakthrough brings comprehensive detection, policy enforcement, and automated response to all MCP based AI operations across the organization.

Xeris Extended Detection and Response System for MCP

Key innovations include:

> ▯ ▯▯▯ ▯▯ ▯ ▯▯ ▯▯▯▯▯▯▯▯▯▯
> ▯▯▯▯▯▯▯▯:
> "I tested Xeris with Brave Search and GitHub. It worked well and securely accessed private repos using Xeris. Great idea and product.""
>
> ▯ ▯▯▯▯ ▯▯ ▯ ▯▯ ▯▯▯▯▯▯▯▯▯
> ▯▯▯▯▯▯▯

• MCP Guard – Provides real time content and behavior inspection of MCP Servers to detect malicious behavior, including prompt manipulation, forged metadata, interference with LLM reasoning, and out of scope execution. Each MCP Server is isolated in a secure sandbox to prevent data leakage, unauthorized communication with other MCPs, or external contact with attacker infrastructure.

• MCP Server Registry and Security Management – Every MCP is vulnerability scanned before installation in the Xeris MCP Gateway. Updates are automatically scanned to prevent malicious code from entering production environments.

• Automated Response and SIEM Integration – Upon detection, predefined responses instantly terminate the attack. Full SIEM integration ensures centralized visibility, case management, and

control within SOC workflows.

Xeris MCP-XDR will be available for customers by end of July 2025. Early birds interested in preview and installation may contact us at info@xeris.ai.

Building on Prior Innovation:

On May 8, 2025, Xeris released the first iteration of its MCP Gateway, enabling enterprises to define and manage multiple MCP Servers with secure user authentication in the cloud. This launch also included an out of the box AI Assistant, allowing corporate users to easily configure tailored AI Assistants, such as a Sales 360 Assistant by enabling Marketing and Sales MCP Servers, or an R&D Assistant combining GitHub, Jira, and Slack MCP Servers.

With the addition of MCP-XDR, Xeris delivers the security layer enterprises have been waiting for, enabling policy enforced, secure use of AI Assistants and Agents that retrieve sensitive data via MCP. This innovation removes one of the major roadblocks to MCP adoption by enterprises, unlocking secure, scalable AI deployments aligned with corporate security standards.

Founders' Statement:
"We created Xeris to solve a problem we kept seeing in every enterprise working with AI Assistants and AI Agents, unsafe, fragmented access to internal tools through multiple MCP Servers. The process was slow, risky, and hard to govern. So we built the Xeris Gateway, a Secured MCP Gateway that centralizes control, enforces policies, and enables safe, fast deployment of AI Assistants and AI Agents."
— Shlomo Touboul, Reffael Caspi, Founders of Xeris

About Xeris
Xeris Inc. and Xeris Ltd. were founded in 2024 to address the growing security challenges of Generative AI adoption in the enterprise.
Xeris secures the future of enterprise AI by providing the industry's first Secure MCP Gateway and MCP-XDR system. Built to protect AI Assistants and AI Agents at scale, Xeris enables organizations to centrally manage access, enforce policies, and respond to threats, bringing control and compliance to AI-powered operations.

Shlomo Touboul
Xeris Inc.
+972 544227780
info@xeris.ai
Visit us on social media:
LinkedIn