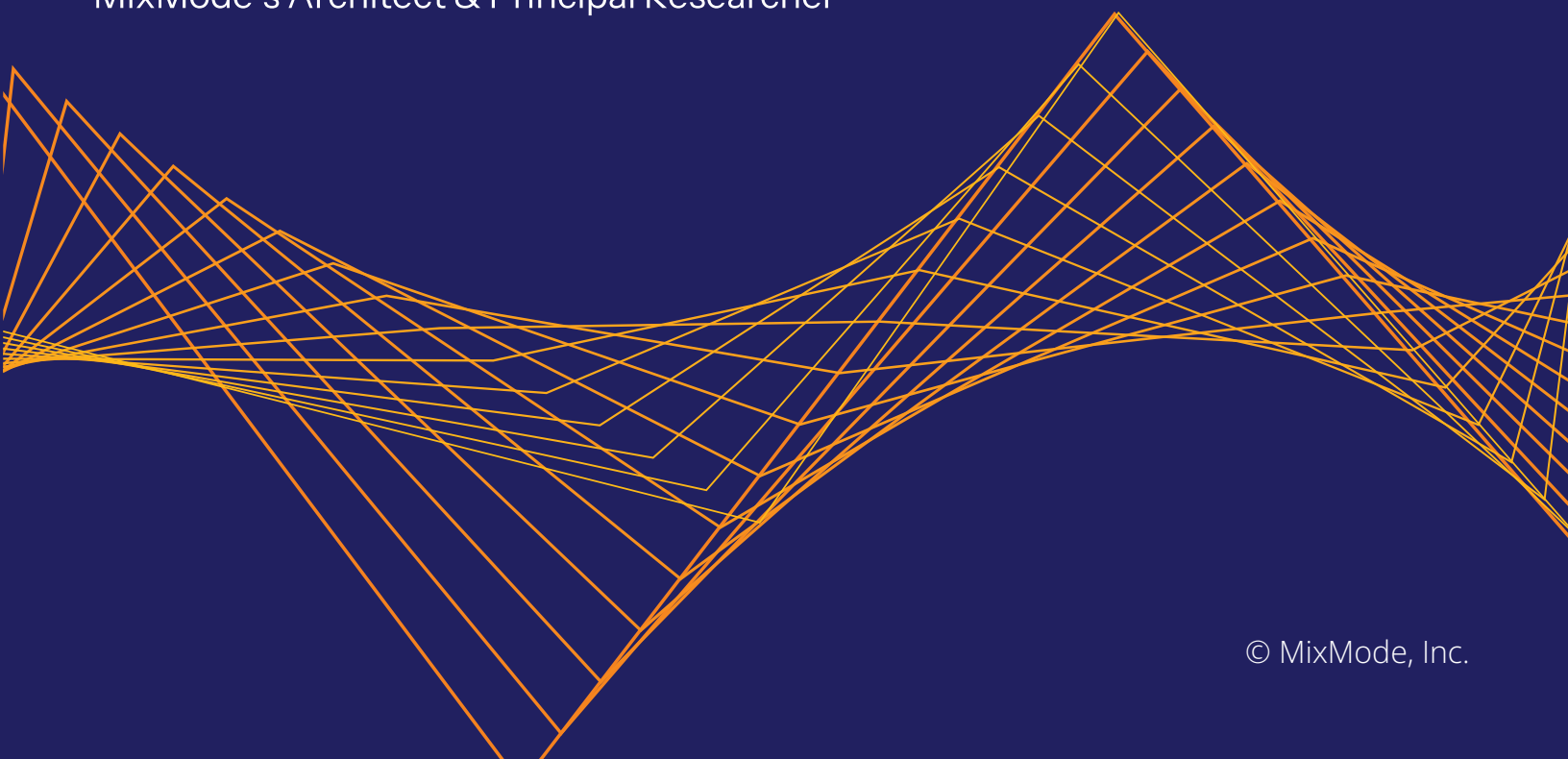
MixMode®

THREAT REPORT

Safeguarding SAP Systems Amid Rising Financial Fraud and Economic Stress

Michael Yelland
MixMode's Architect & Principal Researcher



In today's financial and economic world, applications like SAP that manage business finances are vital. These systems process billions of transactions daily, making them prime targets for errors, exploits, and data alterations, all under intense scrutiny.

Economic stress, such as inflation or market volatility, fuels fraud attempts, as financial pressures push insiders and external actors to exploit vulnerabilities.

Recent vulnerabilities targeting financial software, including SAP, highlight the need for robust cybersecurity. Late April 2025 advisories revealed critical risks that could enable financial fraud, such as unauthorized transactions or data manipulation.

This threat report explores these risks, indicators of attack, and how MixMode's AI-driven solutions simplify SAP security, drawing analogies from cloud security principles.

The Rising Threat Landscape

Economic stress increases fraud, with reduced oversight creating opportunities for financial crime. SAP systems, handling critical financial modules like FI/CO, are vulnerable due to their role in processing massive transaction volumes. A notable case saw a company file for bankruptcy after an SAP breach disrupted financial operations, showing the severe impact of such attacks. Recent reports also note a surge in ransomware targeting SAP, amplifying financial risks.

Recent SAP Vulnerabilities and Exploits (April 21–27, 2025)

In late April 2025 a critical zero-day vulnerability in SAP NetWeaver, known as CVE-2025-31324 (CVSS score: 10.0), was disclosed. This flaw in the SAP Visual Composer component allows attackers to upload malicious files, like JSP webshells, leading to full system compromise. SAP issued an emergency patch, but exploitation attempts continue. Earlier vulnerabilities from April 2025, including code injection flaws in SAP S/4HANA and Landscape Transformation, could also enable fraud by allowing attackers to manipulate financial records, redirect payments, or alter ledgers.

Financial Risks and Their Magnitude

Financial risks from SAP exploits are significant. Fraud can cost businesses millions annually, with SAP systems contributing heavily due to their financial management role. The bankruptcy case illustrates how a single breach can lead to massive losses, including operational disruptions and compliance issues. Rising ransomware and dark web activity targeting SAP further elevate these risks, making robust security essential.

Indicators of Risk

- Unpatched Systems: Outdated SAP versions or missing patches increase vulnerability.
- Misconfigurations: Poorly secured interfaces or weak access controls heighten exposure.
- High Transaction Volumes: Large transaction flows amplify the impact of fraud.
- Economic Stress: Financial pressures drive more fraud attempts.
- Insider Threats: Employees may manipulate financial modules for personal gain.
- Third-Party Risks: Vendor dependencies introduce additional vulnerabilities.

Indications of Attack

- Unusual File Uploads: Malicious files in SAP NetWeaver directories signal active exploits.
- Suspicious Network Traffic: Unexpected data spikes or odd-hour communications suggest data theft.
- Unauthorized Access Attempts: Multiple login failures or new admin accounts indicate attacks.
- Anomalous Transactions: Rapid sequences or high-value outliers point to fraud.
- System Changes: Unauthorized configuration tweaks suggest compromise.

Indicators of Compromise (IoCs)

- Malicious Files: JSP webshells in SAP NetWeaver directories.
- Suspicious IPs: Connections to unknown or risky IP addresses.
- Backdoors: Webshells deployed for persistent access.
- Anomalous Logs: Logs showing unauthorized access to financial data.
- Attack Tools: Use of tools like Brute Ratel for evasion.

Proactive Defenses for SAP Systems

- Patch Promptly: Apply emergency patches for recent vulnerabilities.
- Monitor Actively: Use SAP APIs to track transactions and logs in real-time.
- Use AI Tools: Deploy AI to detect anomalies like irregular cash flows.
- Secure Access: Enforce strong role-based access controls.
- Assess Regularly: Scan for vulnerabilities and IoCs.
- Train Staff: Educate employees on fraud and security risks.

MixMode

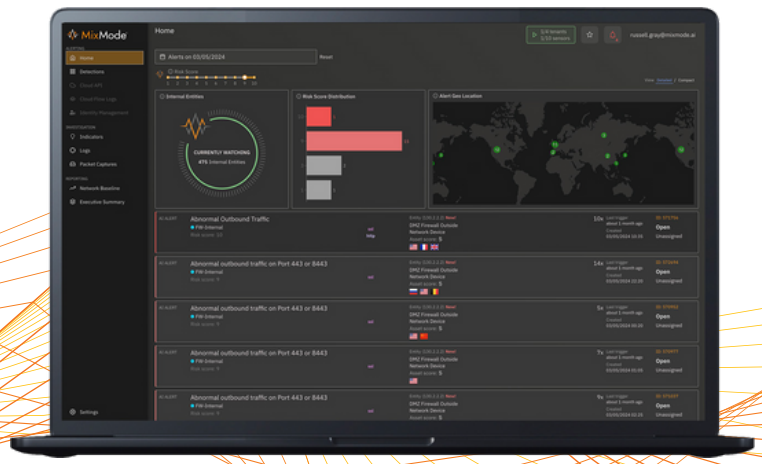
As a MixMode client, you can defer many SAP security concerns to MixMode's third-wave AI monitoring, which simplifies the complex world of accounting software security. Drawing from cloud security principles, MixMode provides out-of-band visibility for SAP cloud environments, much like securing multi-tenant cloud platforms.

Just as cloud security emphasizes real-time monitoring, encryption, and shared responsibility, MixMode ensures SAP systems are protected by analyzing data flows, detecting anomalies, and maintaining compliance without needing deep system access.

Let MixMode help you understand the who, what, when, and relevance of deviations in your SAP environment with these streamlined offerings:

- Real-Time Log Analysis: Ingests SAP transaction and audit logs via APIs, detecting anomalies like unauthorized uploads or rapid transactions instantly.
- AI-Driven Threat Detection: Uses self-learning AI to identify fraud patterns, such as circular payments or insider threats, by adapting to your SAP's normal behavior.
- Out-of-Band Monitoring: Operates independently of SAP, reducing compromise risks and flagging IoCs like malicious IPs or backdoors.
- Simplified Insights: Delivers clear dashboards showing who initiated actions, what was changed, when it happened, and why it matters, prioritizing high-risk events.

MixMode's approach cloud security's focus on agility and scalability, ensuring your SAP systems remain secure and compliant in a dynamic threat landscape.



mixmode.ai