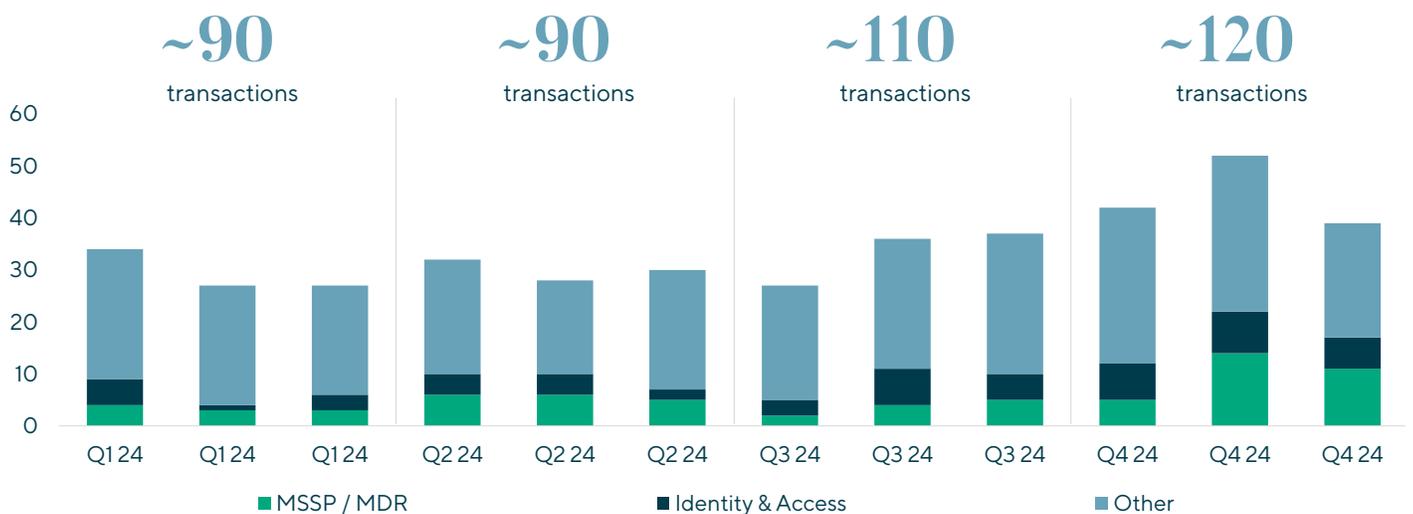
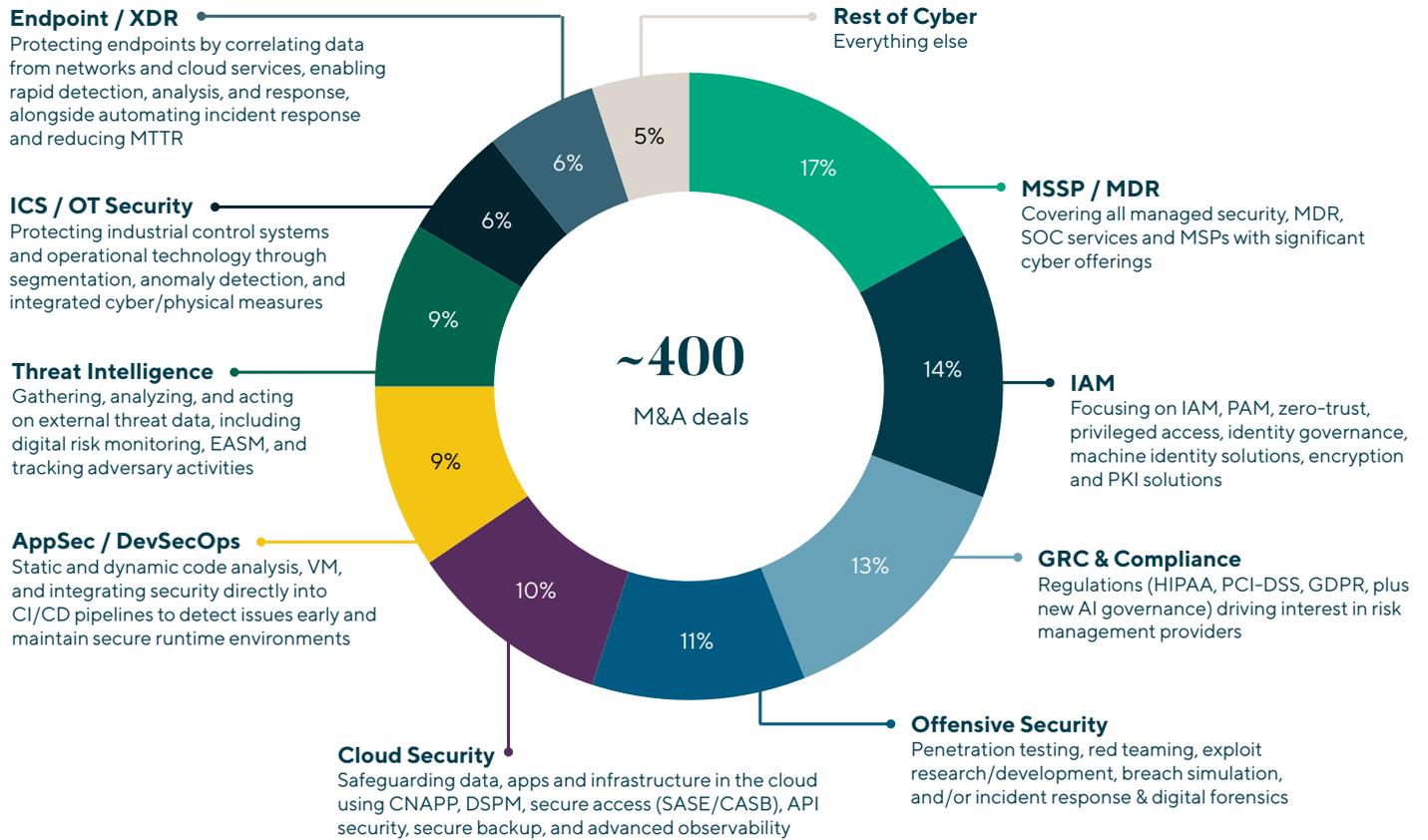


Cyber Roadmap: 2025 and beyond

In 2024, the cybersecurity mergers and acquisitions (M&A) landscape saw significant momentum, particularly in the second half of the year. After the challenges of 2022 and 2023, transaction volume rebounded, with **Identity & Access Management (IAM)**, **Managed Detection and Response (MDR)** and **Managed Security Service Providers (MSSPs)** remaining dominant categories. This ongoing consolidation highlights the strategic importance of these verticals.

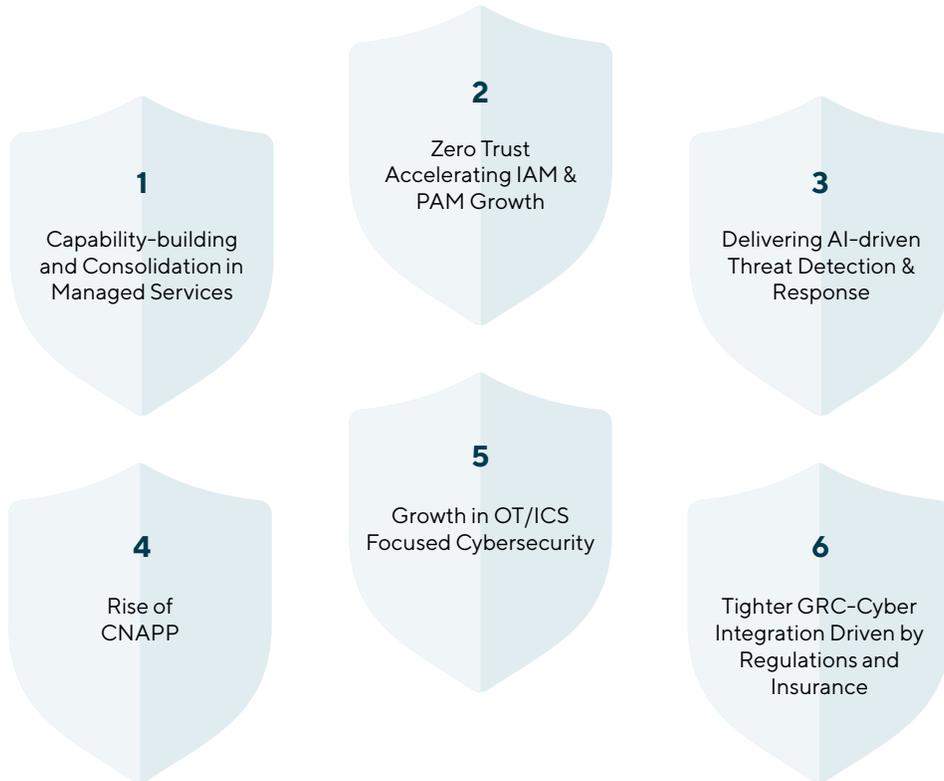


Mapping 2024 Cyber M&A Transactions



The global cybersecurity sector saw approximately 120 transactions closed in Q4 alone, demonstrating strong momentum. Lincoln International's team of European cybersecurity bankers has identified six key themes and consolidation drivers from 2024 that will shape M&A activity across the European cybersecurity sector in the coming quarters.

Six Cyber Themes and Consolidation Drivers



1 Capability-building and Consolidation in Managed Services

Convergence of Security Services and Platforms: Enterprises increasingly demand unified security and IT support, driving acquisitions of MSSPs and MDR providers. By integrating complementary technologies (e.g., asset discovery, vulnerability management, security analytics), providers can deliver centralized extended detection and response (XDR) capabilities across endpoints, networks, identities and cloud workloads.

Cloud-native Security and DevSecOps Integration: As organizations of all sizes adopt hybrid and multi-cloud environments, MSSPs and MDR providers require cloud-native threat detection and response alongside specialized DevSecOps expertise. Smaller, niche players were often targeted for their ability to meet these needs.

Expansion of Industry / Geography-specific Offerings: End-customers in regulated sectors like healthcare, finance and government are driving provider acquisitions for threat intelligence and detection capabilities tailored to their unique compliance requirements. Similarly, cross-border deals were spurred by data sovereignty and regional alignment needs.

PE-led Scalability & Cost Efficiency: Larger MSP / MSSPs backed by external capital acquired strategic targets to scale operations, reduce overhead and invest in capabilities such as zero trust and AI-driven detection. Smaller providers sought mergers to reach the same goals.

2 Zero Trust Accelerating IAM & PAM Growth

“Identity as the Perimeter”: The shift to remote work, hybrid cloud and highly distributed architectures has positioned identity and privileges as “the new perimeter.” Zero trust frameworks anchored by IAM and least-privilege controls mitigate insider threats and lateral movement.

Convergence of IGA, PAM, and CIEM: Acquirers are increasingly seeking a unified identity security stack that spans workforce identity, privileged account protection and entitlement management. M&A activity consequently centered on consolidating Identity Governance and Administration (IGA), Privileged Access Management (PAM) and Cloud Infrastructure Entitlement Management (CIEM) into unified platforms.

Expanding Machine Identities: Beyond human identities, companies are focused on securing machine identities like IoT sensors, RPA bots and cloud microservices to prevent lateral movement attacks. Deals often targeted solutions for ephemeral credentials and dynamic identities in DevOps and containerized microservices environments.

The AI IAM Layer: IAM solutions increasingly leveraged AI-based anomaly detection to detect credential abuse, privilege escalation or unusual behavioral patterns that deviated from established baselines.

3 Delivering AI-driven Threat Detection & Response

AI-enabled Predictive Intelligence: Companies are increasingly using AI to anticipate threats before they manifest. For example, Protect AI’s acquisition of Laiyer AI aimed to shield large language models (LLMs) from adversarial attacks by using historical and real-time data to forecast potential breaches and proactively secure vulnerabilities across digital assets.

Automated Alert Triage and Incident Response: Machine learning allows organizations to sift through thousands of alerts, distinguishing routine activity from high-risk threats like lateral movement or anomalous file access. Automated incident escalation further reduces response times.

Generative AI Security Measures: As businesses rely on generative AI for tasks like customer service and data analysis, security solutions emerged to protect models from threats like prompt injection, data poisoning and model theft. These measures monitor input / output patterns and flag unusual query spikes or subtle behavior changes.

Unified AI Integration Across Security Platforms: Rather than isolated tools, AI integration across platforms enables a holistic security posture, automating cross-layer correlation and response. Notable deals include GitLab’s acquisition of Oxeye to enhance its static analysis with ML-based scanning, and Cloudera’s acquisition of Verta integrated MLOps into its analytics platform.

4 Rise of CNAPP

CNAPP Addresses Cloud Security Holistically: CNAPP solutions combine vulnerability management, runtime protection, misconfiguration scanning and data security into one comprehensive suite rather than operating in silos. CNAPP ensures cloud-native applications are continuously monitored and secured from development through production.

Shift-Left Security: As DevSecOps becomes the norm, CNAPP integrates security early in the development cycle, enabling continuous protection throughout the application lifecycle.

Data Privacy Regulations: Expanding regulations in countries across the world require sophisticated solutions for data discovery, classification and encryption. CNAPP providers increasingly incorporated Data Security Posture Management (DSPM) to meet compliance needs while protecting sensitive data in dynamic cloud environments.

5 Growth in OT / ICS Security & Defense Sector

Critical Infrastructure, ICS, and OT Security: The rising importance of protecting industrial control systems (ICS) and operational technology (OT) was driven by high-profile disruptions in energy, transportation and manufacturing sectors. Governments are enforcing stricter regulations to defend against nation-state attacks and ransomware targeting critical infrastructure. Securing energy grids, water treatment facilities, rail lines and other national assets has intensified the demand for specialized security solutions and are driving significant investment in robust OT security measures.

Race to Acquire Specialized Capability: Defense contractors and niche OT security firms actively pursued strategic acquisitions to develop advanced detection, segmentation and zero trust capabilities for industrial environments. Companies like Parsons, GDIT and Accenture Federal are ramping up acquisitions to deliver turnkey ICS cybersecurity solutions tailored for government agencies.

“

The rising importance of protecting industrial control systems (ICS) and operational technology (OT) was driven by high-profile disruptions in energy, transportation and manufacturing sectors.

6 Tighter GRC-Cyber Integration Driven by Regulations and Insurance

Evolving Cyber Regulations and Data Protection: Expanding industry-specific and privacy regulations are creating overlapping mandates that drive demand for Governance, Risk, and Compliance (GRC) solutions. These platforms help avoid fines and reputational risks while automating regulatory tracking—especially for multinationals handling sensitive data such as payments. This drives demand for automated regulatory tracking solutions.

	Expanding Privacy Laws	Industry-Specific Rules
	General Data Protection Regulation (GDPR)	Network and Information Security Directive 2 (NIS2) Payment Services Directive 2 (PSD2)
	The California Consumer Privacy Act (CCPA)	Health Insurance Portability and Accountability Act (HIPAA) Payment Card Industry Data Security Standard (PCI-DSS)

Complex Third-Party and Supply Chain Risk: The increasing prevalence of breaches compelled enterprises to continuously monitor third-party cyber risks. GRC solutions equipped with embedded vendor risk assessments help minimize exposure—for example, financial services firms can track encryption standards and receive alerts for compliance lapses.

Convergence of Cyber Insurance and Risk Management: Insurers now require stricter controls for cyber coverage, and robust security controls and documentation are critical. GRC platforms centralize information including policies, incident response plans and compliance records, improving access to cyber insurance and potentially lowering premiums.

AI Governance and Emerging Regulatory Obligations: Emergent AI guidelines around fairness, bias and generative outputs introduced additional compliance layers. GRC platforms can track data handling practices and model training processes while ensuring adherence to regulations. For instance, companies using AI chatbots may rely on GRC tools to document data handling practices, model training processes and adherence to emerging regulations.

Looking Ahead with Lincoln

As we move into 2025, the European cybersecurity sector will continue to evolve, driven by regulatory demands, enterprise priorities, macroeconomic tailwinds and technological innovation. Lincoln International's team of dedicated European cybersecurity bankers is uniquely positioned to navigate complex situations and deliver value-add advisory services to clients.

Continued Rise of AI-First Security Platforms	<ul style="list-style-type: none">• Use of AI systems to enable proactive defenses expected to become the norm• Routine SOC tasks become automated (correlating data from EDR, SIEM and cloud logs), slashing MTTR• Large vendors will acquire specialized AI startups to integrate cutting-edge threat detection• Premium valuations for "AI-first" firms: strategic buyers value innovative solutions in challenging markets
Zero Trust 2.0 & Identity-Centric Ecosystems	<ul style="list-style-type: none">• Full-stack zero trust will converge IAM & PAM (identity threat detection, device posture, JIT access)• Surge in non-human identities (IoT, RPA, microservices) drives next-gen identity management deals• Consolidation as large players fill gaps in ephemeral and machine identity management
Cloud Sec Matures to Full Data Sovereignty	<ul style="list-style-type: none">• CNAPP merges with DSPM for unified runtime protection, compliance and data security• Tightening data localization (Europe/APAC) drives demand for sovereign cloud and edge security• M&A focuses on cross-border data flow, encryption, zero trust segmentation and DSPM tools
ICS / OT Security Demand Accelerates	<ul style="list-style-type: none">• Nation-state and ransomware attacks drive focus on critical ICS/OT infrastructure• Need for specialized solutions for legacy ("brownfield") ICS assets (old hardware, proprietary protocols)• Defense contractors/integrators drive M&A; premium for unidirectional gateways and advanced OT anomaly detection
GRC and Privacy: New AI Regs Spur Growth	<ul style="list-style-type: none">• EU AI Act and emerging US guidelines will push continuous AI auditing (transparency, bias, accountability)• Large GRC platforms acquire/partner with AI risk startups for algorithmic risk scoring & model auditing• PE keen on subscription-based compliance solutions (finance, healthcare), driving unified risk platforms

Connect with us today to explore the opportunities and trends shaping the future of cybersecurity.

Ready to discuss the opportunities ahead for you?

Connect with a senior professional at connect@lincolninternational.com