Deloitte.

Reimagining modern Enterprise Resource Planning (ERP) security

ERP platforms have adopted innovations like cloud, big data, and artificial intelligence (AI)—creating the opportunity to rethink ERP security for today's technology-driven environment.

The evolution of ERP systems is being shaped by AI, which automates tasks like invoice processing, expense approvals, and supply chain management. Predictive analytics and intelligent insights can help forecast demand, manage cash flow, and anticipate workforce needs. Machine learning (ML) models identify workforce risks and trends, while conversational and generative artificial intelligence (GenAI) powers chatbots and virtual assistants for human resources, finance, and procurement support.

Security is also advancing, with AI-driven analytics monitoring user activity to detect unusual behavior and threats in real time. ERP environments becoming more complex requires unified security management, strong controls over application programming interfaces (APIs), and ongoing third-party risk oversight to maintain system integrity.

The future of ERP: Embracing AI

A blueprint for ERP security and underlying services/processes: As organizations build an ERP security strategy and roadmap to enable AI within their organization, they will need to evaluate tools and technologies against the emerging set of capabilities.

Identity and access management	Data privacy and protection	Cyber governance and strategy	Application security	Monitoring and response	Operational security	Internal controls	Infrastructure security	Business continuity and IT disaster recovery
🟩 Governance	🟦 Data classification and discovery	🟦 Security policies	🟦 Role-based access control (RBAC)	🟦 Audit logging	🟦 Operating procedures	🟦 Business process controls	🟩 Operating systems	🟩 Disaster recovery
🟦 Privileged access management (PAM)	🟦 Data protection	🟩 Roles and responsibilities	🟦 Segregation of duties (SoD)	🟩 Monitoring controls	🟩 Operating model	🟦 IT general controls	🟦 ERP database security hardening	🟩 Operational outages
🟩 Single sign-on (SSO) and multi-factor authentication (MFA)	🟩 Data life cycle management	🟩 Risk management	🟦 ERP vulnerability management	🟦 Security information and event monitoring	🟩 Reengineering and optimization	🟦 Interface controls	🟩 Network security and segmentation	🟩 Third-party disruptions
🟦 Identity life cycle management	🟩 Data loss prevention	🟦 Cyber metrics	🟩 Secure software development life cycle (SDLC)	🟩 Life cycle create, update, and revoke		🟦 Data conversion controls	🟩 Endpoint security	🟩 Business continuity plan
🟩 Integration		🟩 Security awareness and training	🟩 Change management	🟦 Threat intelligence		🟦 Software development life cycle controls	🟩 Digital key management	🟦 Incident response
🟦 Access certification			🟩 Patch management			🟦 Continuous controls monitoring	🟩 Cloud access security brokers (CASB)	
🟦 Self-service portal			🟩 API security			🟩 Risk and control management	🟩 Infrastructure vulnerability management	
🟩 Authoritative sources			🟦 Non-production access					
			🟩 License management					

LEGEND

🟦 **Capabilities evolving to include AI**

🟩 **Capabilities not yet AI-enabled**

Takeaways

ERP security AI enablement is early stage and evolving rapidly as more ERP companies look to redesign their platforms using an agentic model with AI training models at the core of their software design paradigm.

These capabilities depend on training data to drive solution maturity; organizations need to establish the right procedures to support and maintain at scale.

Connect to accelerate

Contact our leaders to dive deeper into the blueprint and reimagine what's possible for your organization.

Mark Nicholson
Principal
Cyber AI
GTM Leader
Deloitte & Touche LLP
manicholson@deloitte.com

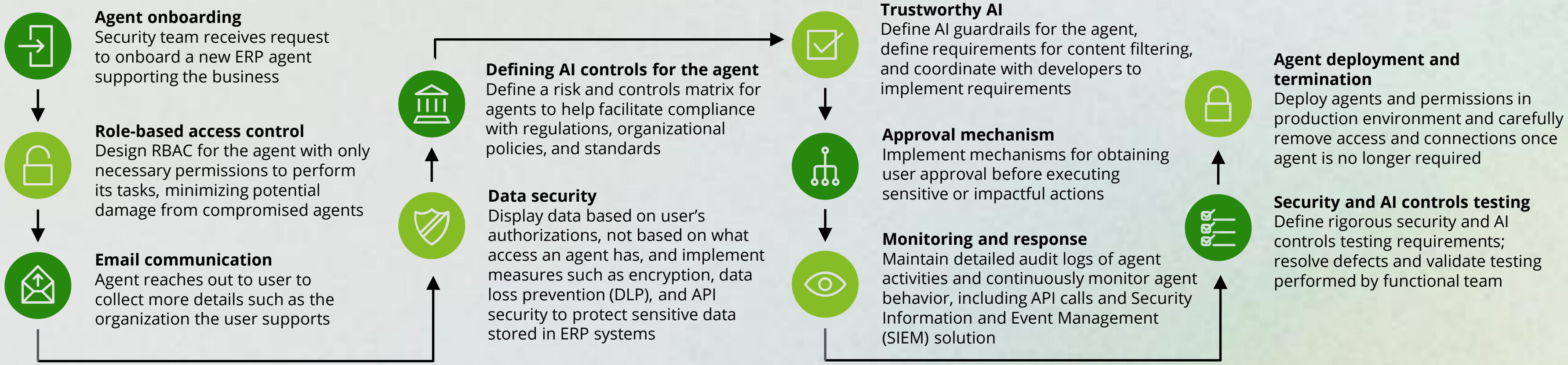
Naresh Persaud
Principal
AI Transformation Leader
Deloitte & Touche LLP
napersaud@deloitte.com

Sachin Singh
Managing Director
ERP Security Leader
Deloitte & Touche LLP
sachisingh@deloitte.com

Steve Ruzzini
Senior Manager
Cyber AI GTM
Activation Lead
Deloitte & Touche LLP
sruzzini@deloitte.com

ERP for AI: Security controls per application for securing AI

As ERP solutions incorporate more AI and agentic capabilities, security teams should consider adjusting their considerations to secure new risks introduced by these capabilities.



Agent onboarding
Security team receives request to onboard a new ERP agent supporting the business

Role-based access control
Design RBAC for the agent with only necessary permissions to perform its tasks, minimizing potential damage from compromised agents

Email communication
Agent reaches out to user to collect more details such as the organization the user supports

Data security
Display data based on user's authorizations, not based on what access an agent has, and implement measures such as encryption, data loss prevention (DLP), and API security to protect sensitive data stored in ERP systems

Defining AI controls for the agent
Define a risk and controls matrix for agents to help facilitate compliance with regulations, organizational policies, and standards

Trustworthy AI
Define AI guardrails for the agent, define requirements for content filtering, and coordinate with developers to implement requirements

Approval mechanism
Implement mechanisms for obtaining user approval before executing sensitive or impactful actions

Monitoring and response
Maintain detailed audit logs of agent activities and continuously monitor agent behavior, including API calls and Security Information and Event Management (SIEM) solution

Security and AI controls testing
Define rigorous security and AI controls testing requirements; resolve defects and validate testing performed by functional team

Agent deployment and termination
Deploy agents and permissions in production environment and carefully remove access and connections once agent is no longer required

AI for ERP: Functional uplifts to achieve greater efficiency

Relying on manual efforts for ERP processes can lead to inconsistencies, increased risk of human error, and higher operational costs. Automating and standardizing security practices facilitates more consistent protection, reduces vulnerabilities, and accelerates delivery timelines.

ERP domains	Uplift approach	Resulting impact
Identity and access management	Automates access provisioning processes and periodic access certification	**Streamlined identity management and enhanced security**
Data privacy and protection	Recommends data security and handling related controls	**Strengthened data security and reduced exposure to breaches**
Operational security	Provides faster, more thorough, efficient, and improved security posture	**Improved operational efficiency and proactive threat management**
Infrastructure security	Recommends and fixes configuration autonomously and automatically	**Strengthened infrastructure security and improved resilience against attacks**
Controls and compliance	Enables real-time compliance monitoring and automates audits for greater accuracy and efficiency	**Enhanced compliance, reduced regulatory risk, and faster, more accurate audits**
Monitoring and response	Continuously monitors systems, detects threats, and triggers automated responses via playbooks	**Faster threat detection, quicker response, and reduced business impact from security incidents**

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication. As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com /us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.