DELL Technologies

AI Security and Resilience Services

Trust your use of AI

Addressing the Challenges of AI Adoption

Artificial Intelligence (AI) is a game-changer for businesses, enabling groundbreaking innovation and faster decision-making. But with great potential comes significant challenges. AI adoption introduces unique concerns in security, trust, and compliance, placing new pressures on organizations. At Dell Technologies, we've reimagined how AI security should work. Our approach uniquely integrates data management, infrastructure security, and AI model protection to offer a comprehensive, tailored solution. Whether you're new to AI or scaling existing solutions, our end-to-end services are designed make AI adoption faster, safer, and more reliable.

Security is Not Just IT's Job

Modern AI-related security requires collaboration across teams. AI security is a team sport, requiring input and decision-making from across your organization. Traditional siloed IT operating models won't work in this evolving landscape. Our unique approach incorporates data, infrastructure, applications, and models into a single cohesive strategy that adapts to your specific business needs, offering a holistic solution that helps you stay ahead.

Addressing AI's Unique Security Challenges

AI adoption introduces complex security and compliance considerations that can jeopardize its potential benefits, such as:

- Data breaches and loss of intellectual property (IP) due to inadequate data protection or unauthorized access.
- AI-powered threats such as adversarial attacks, model manipulation, or training data poisoning.
- Availability challenges for now-critical AI tools, like support agents, to be continuously operational.
- Third-Party Supply Chain Vulnerabilities that stem from interconnected systems.
- Expanding Attack Surfaces as AI applications scale across hybrid and multicloud environments.
- While not purely a security concern, hallucinations can mislead users

Key Benefits

Enhanced Trust & Transparency: Safeguard data, intellectual property, and AI integrity to maintain confidence among stakeholders.

Operational Resilience: Keep your mission-critical AI systems stay operational and resistant to threats.

Regulatory Compliance: Help meet your industry and government regulations to avoid costly penalties and reputational damage.

Scalable Solutions: Deploy adaptable AI security measures that grow with your organization and its technology stack.

Expert Support & Guidance: Work with proven security experts to tailor your solution and deliver measurable outcomes.

End-to-end services to deliver a tailored security architecture

Our Dell-developed security architecture is designed to meet your unique needs, providing a flexible and dependable foundation. It seamlessly integrates with the Dell AI Factory, activates zero trust principles, and incorporates expertly integrated partner technologies to drive secure, forward-thinking innovation.

AI Models and Applications

Data

Infrastructure

	Features
Advise Align your AI security with organizational needs and compliance requirements	• **Security and Resilience for AI Advisory Services** include business and technical workshops to develop a comprehensive security and availability strategy • **CISO Advisor for AI** provides a virtual CISO who is an expert in AI to kick start your AI security strategy • **Data Security for AI** helps reduce data security threats and risks to your data
Implement Design and implement security software to increase visibility of AI stack	• **Security Software Design and Configuration** to integrate tools which protect access management, applications and networks
Manage Enable deep visibility across the stack to quickly detect and respond to threats	• **Managed Detection and Response (MDR)** for 24/7 threat detection across data, infrastructure, applications, and models • **Managed AI Firewall** imposts an isolated set of AI-based guardrails and inspects prompts and outputs for policy compliance • **Penetration Testing for AI** to simulate adversarial attacks and uncover weaknesses • **Incident Response and Recovery Services** to help you recover fast and get back to business with minimal interruption

Build a Secure AI Future with Confidence

Dell's AI Security and Resilience services are crafted to address novel risks associated with integrating AI into your organization. Built to work alongside your teams as you onboard AI as quickly as possible, our services provide expertise to guide in strategic planning, solution implementation and managed security services to ease operational burdens so you can innovate securely with AI.

Explore Dell Security and Resiliency Services

Contact a Dell Technologies expert

Join the conversation with #DellTechnologies

DELL Technologies