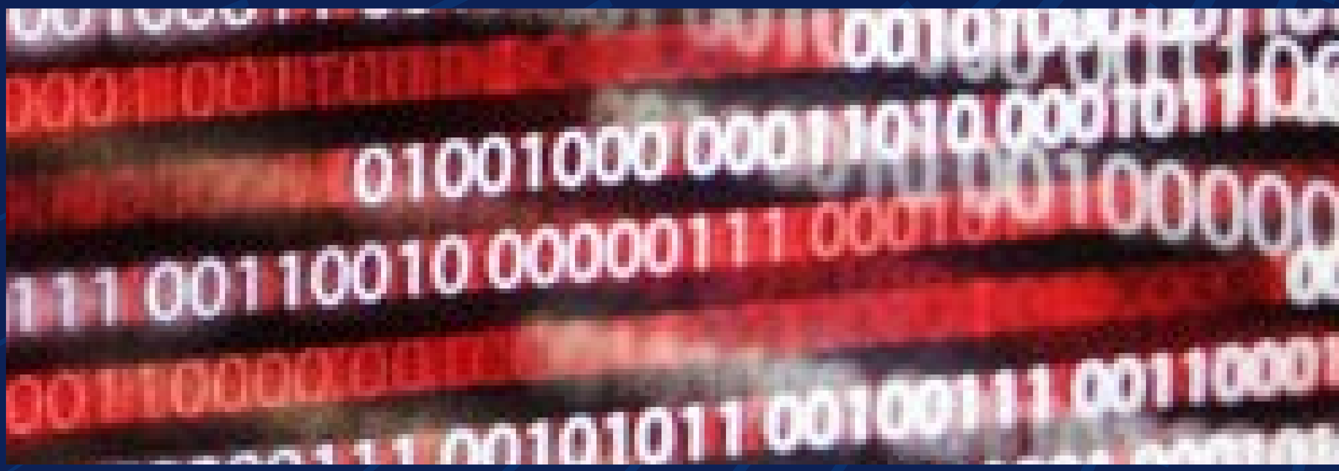
DELL Technologies

The Cybersecurity Mythbusters:

Debunking AI Security Myths



AI is transforming industries, but when it comes to securing AI, many organizations fall victim to myths that make it seem more complex than it really is. The truth? Protecting AI systems doesn't require starting completely from scratch—applying existing cybersecurity principles to AI's unique challenges goes a long way.

At Dell Technologies, we understand the architecture behind AI and can help you adapt your current solutions to fit this new framework. Let's break down the most common myths surrounding AI security and uncover the truths to help you secure your systems effectively.

Myth 1: "AI systems are too complex to secure."

The Truth: It is true that AI creates new cybersecurity risks like prompt injection, data manipulation, and sensitive information disclosure just to name a few. Additionally, Agentic AI systems also come with a broader attack surface, as they can be exploited to manipulate outcomes or escalate privileges.

That said, while it's critical to recognize these vulnerabilities and implement security measures to protect AI systems from both traditional and AI-specific threats, the risks can be managed and AI models can be secured. It's important to keep in mind that AI systems require significant amounts of data as inputs and create large amounts of data as outputs. That puts data protection front and center as one of the key security strategies, along with:

- Zero trust principles such as identity management, roles-based access, and continuous verification.
- Regular penetration testing and vulnerability management to identify weaknesses.
- Logging and auditing to validate data inputs and outputs

Myth 2: "None of my existing tools will secure AI."

The Truth: AI security isn't about starting over—it's about working smarter the tools you already have. Most existing cybersecurity tools can be adapted to secure AI systems effectively. At its core, AI is one more workload in your arsenal driving your business, albeit one with unique characteristics. Foundational cybersecurity practices, such as identity management, network segmentation & monitoring, endpoint protection, and data protection, remain essential for safeguarding AI environments. The key is adapting these practices to address specific AI challenges, such as protecting training data, securing algorithms, and mitigating risks like adversarial inputs.

A strong defense begins with good cyber hygiene—such as system patching, access control, and vulnerability management. What's important is tailoring these practices to address AI-specific risks. With AI-focused strategies integrated into your current security approach, and the right tools, AI security becomes manageable and effective.

It is important to point out, however, that updated hardware can play a critical role in combatting cyberattacks. For example, modern AI PCs create a strong first line of defense against a major attack vector: Endpoints. With Windows 10 support ending, outdated PCs become a risk. Furthermore, Windows 11 requires Trusted Platform Module (TPM) version 2.0, a security chip that helps with encryption, secure boot, and protection against firmware attacks. Many older PCs either don't have TPM at all or only support an older version. Dell offers secure commercial AI PCs with these enhancements built in.

The same goes for AI infrastructure like servers and storage. The Dell AI Factory includes hardware that is optimized for AI security and contains a number of built in security features ranging from a secure supply chain to data immutability to isolation and encryption.

Myth 3: "AI security is only about protecting data."

The Truth: AI security extends beyond basic data protection—it involves safeguarding the entire AI ecosystem, including models, APIs, outputs, systems and devices. As AI becomes more integrated into critical applications, the risks associated with its misuse or exploitation escalate. Without robust security measures, AI models can be tampered with to generate harmful or misleading outputs, APIs can be exploited to gain unauthorized access to sensitive systems, and outputs can inadvertently expose private or confidential information.

Comprehensive AI security requires a multi-layered approach. This includes protecting models from adversarial attacks that attempt to manipulate input data to deceive AI systems, securing APIs with strong authentication methods to prevent unauthorized use, and **continuously monitoring outputs** for unusual or suspicious patterns that could signal an attack or malfunction. Effective AI security not only ensures the integrity and reliability of AI systems but also builds trust with users and stakeholders by mitigating the risks of malicious use or unintended consequences.

Myth 4: "AI doesn’t need human oversight."

The Truth: Governance and human oversight are critical to ensuring that AI systems operate ethically, predictably, and in alignment with human values. Advanced AI systems, particularly agentic AI with autonomous decision-making capabilities, introduce unique challenges that demand robust safeguards. Without proper oversight, these systems could deviate from intended goals or exhibit unintended behaviors that may pose risks.

To address this, it is essential to establish clear boundaries, implement layered control mechanisms, and ensure ongoing human involvement in critical decision-making processes. Regular audits, transparency in AI operations, and thorough testing can further enhance accountability and trust, helping to prevent misuse and promoting the responsible deployment of AI technologies.

Best Practices for Strengthening AI Security

To close AI-specific security gaps, organizations need to adopt a proactive and strategic approach. Here are 10 best practices to secure your AI systems:

Layered Security Architecture:
Use segmentation, firewalls, and strong authentication to protect your infrastructure, software, and data at every layer.

Secure the Supply Chain:
Implement a strong supplier management program. Audit vendors andthird-party components, validate integrity, and rely on signed code to prevent ulnerabilities in the AI development lifecycle.

Protect Training Data and Models:
Safeguard against poisoned data, adversarial inputs, and other threats by monitoring data integrity and applying robust validation tools.

Tighten Access Controls:
Enforce least privilege principles, implement role-based access control (RBAC), rotate credentials regularly, and audit permissions to prevent unauthorized access.

Secure APIs:
Use strong authentication protocols (like OAuth 2.0), enforce HTTPS encryption, and regularly update APIs to close potential vulnerabilities.

Monitor and Validate AI Outputs:
Use anomaly detection, logging, and alerts to monitor for unusual patterns or harmful behaviors in AI outputs.

Plan for Resilience:
Regularly back up data and test disaster recovery plans to minimize downtime and ensure quick recovery in the event of a breach.

Implement Robust Encryption:
Encrypt sensitive data at rest and in transit using strong algorithms, and securely manage and rotate encryption keys regularly.

Conduct Regular Security Audits and Penetration Testing:
Frequently assess systems for vulnerabilities and use penetration testing to uncover risks before they can be exploited.

Train Staff on AI Security Best Practices:
Regularly train your team on secure development, threat recognition, and maintaining strong security practices to prevent breaches.

Dell's Value Proposition: Practical AI Security Solutions.

AI security might seem complex, but it's not as daunting as it appears. The truth? Securing AI isn't so different from securing your existing workloads—it's about understanding the architecture and applying the right strategies. That's where Dell Technologies comes in.

We demystify AI security by leveraging your current solutions and seamlessly integrating them into AI-focused architectures. We tackle challenges like prompt injection, API abuse, and adversarial attacks without requiring a complete infrastructure overhaul.

Dell's expertise lies in cutting through the myths around AI security and showing how achievable it really is. Whether you're just beginning your AI journey or want to enhance your defenses, we'll help you protect your investments, secure your systems, and build a resilient digital future—confidently and effectively. Let's simplify AI security, together.

Dell products and solutions that can help

Featured Dell Solution	Description
Dell AI Factory	Dell AI Factory secures AI workloads through a secure supply chain, ensuring trusted infrastructure from development to deployment. With features like data immutability, isolation, and encryption, it safeguards sensitive models and datasets, defends against cyber threats, and enables scalable, efficient, and seamless AI operations in dynamic, data-driven environments.
Cyber Resilience	PowerProtect secures AI workloads with advanced features like immutability and isolation, ensuring data integrity and protection against cyber threats. It offers end-to-end encryption and anomaly detection while enabling rapid recovery to minimizes downtime.
Dell Trusted Workspace (Endpoint Security)	A combination of built-in and optional add-on capabilities designed to secure commercial AI PCs and AI workloads running on them. Built with secure supply chain practices, built-in capabilities include SafeBIOS and SafeID with TPM. Optional add-ons include Secured Component Verification, SafeID with ControlVault, and partner software CrowdStrike and Absolute to maximize workspace security.
AI Security Advisory Services	A suite of services that can help you develop and implement a comprehensive AI security strategy. Offerings include advisory services, AI vCISO, and data security planning.
Managed Security Operations for AI	Enables deep visibility across the stack to quickly detect and respond to threats. Capabilities include Managed Detection and Response, Managed AI Guard, Penetration Testing for AI, and Incident Response and Recovery Services.
Security Software Integration	Design, install and configure security tools which protect access management, applications, networks, clouds and more.

Learn how to address some of today's top cybersecurity challenges at **dell.com/cybersecuritymonth**

DELL Technologies