WHITE PAPER

A Pragmatic and Resilient Approach to AI

By Pranay Ahlawat,
Commvault Chief Technology and AI Officer

Executive Summary

While businesses strive to unlock the promise of artificial intelligence (AI), its successful application to real problems has been mixed. Unlike the progression of other new technologies, the adoption of AI has been complicated not just by the overwhelming hype, but also by its rapid evolution.

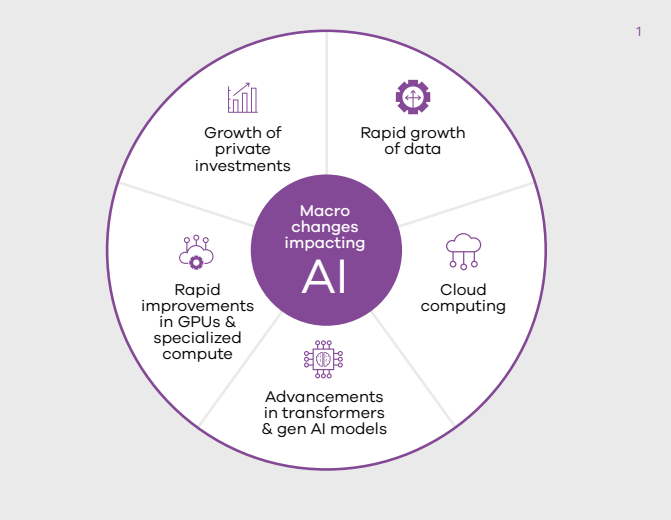
In essence, the transformative power of AI is there, but it has yet to be fully realized. This report looks beyond the hype to help you align your strategic goals and AI investments with pragmatic approaches, while also enabling your organization's data and business to remain resilient and continuous.

CUTTING THROUGH THE AI HYPE

Today's modern approach to AI is the result of several interrelated, iterative innovations. Advances in cloud computing and with AI platforms, services, and APIs are democratizing the vast computing power and storage necessary to run complex AI models. Distributed systems and advanced big data architectures have evolved to provide remarkable scalability and low-latency analytics.

Companies like NVIDIA developed massively powerful GPUs optimized for deep learning to accelerate large-scale model training. The development of transformer architectures and large language models has not only revolutionized human-computer interaction but also enabled the resolution of a new class of problems in design and optimization, thereby paving the way for the advent of artificial general intelligence.

Together, these groundbreaking advancements exploded the boundaries of AI, fueling optimism, experimentation, and the race to invest and implement AI solutions. However, to date, the hype and enthusiasm have been met with mixed results.



There are three reasons for this:

1. **Rapid technological advancement.** The fast pace of technological change makes it difficult for enterprises to keep up, often leading to a mismatch between available technology and organizational capabilities.
2. **Business process transformation.** Organizations need to transform their business processes and enhance cyber resilience, not just focus on technology. AI requires a holistic approach, including changes in culture, data management, and governance.
3. **Evolving technology and use cases.** Both generative AI and traditional ML are still evolving, resulting in notable errors and new threat vectors. This ongoing evolution can introduce unexpected issues that organizations are not prepared to handle.

AI adoption in 2024: **74%** of companies struggle to achieve and scale value.[1]

For instance, McDonald's AI-powered Drive Thru ordering system faced significant challenges, leading to customer frustration and the eventual termination of the project.[2] An inaccurate and potentially libelous finding by Grok, an AI chatbot, raised concerns about the reliability risks of AI.[2] And Uber's autonomous vehicle program was hit head-on with regulatory and safety concerns.[3] These challenges have forced companies to temper their ambitions and reconsider their strategies.

1 Boston Consulting Group, AI Adoption in 2024: 74% of Companies Struggle to Achieve and Scale Value | BCG, October 24, 2024.
2 CIO, 12 famous AI disasters, October 2, 2024.
3 Stanford Law School Blogs, Uber Self-Driving Cars, Liability, and Regulation - Legal Aggregate - Stanford Law School, March 20, 2018.

MAKING AI REAL

Executives in various industries are considering AI's disruptive potential and the significant value of its transformative use cases. However, organizations must take a practical and flexible approach to leverage AI effectively and get value from the investments.

They should invest in transformative "alpha" use cases, like new product introductions, while balancing them with short- and medium-term bets that offer clear ROI and established adoption patterns. This will help an organization fund its journey and remain economically competitive. After all, resources and talent are not infinite, so you must remain pragmatic.

Some short- and medium-term initiatives include:

- **Automate time-consuming, repetitive, and routine tasks.** AI-driven robotic process automation has enabled numerous organizations to achieve significant cost savings and operational efficiencies in finance, HR, and customer service.
- **Augment decision-making.** Leveraging AI-driven data insights, decision makers make more informed choices across various sectors. For example, some healthcare professionals use AI to help analyze patient data to diagnose conditions, identify anomalies, and recommend treatments.
- **Enhance customer experiences.** In addition to offering instant, 24/7 customer support, AI-driven chatbots can enhance customer experiences with personalized, efficient, and responsive services.

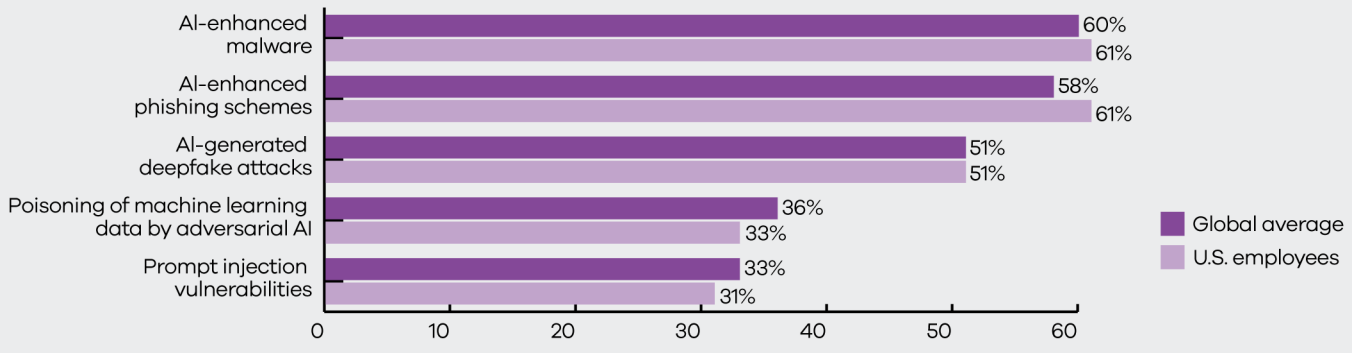
To be successful at this stage, organizations must strategically align their business and outcomes; adopt agile processes to adjust to the ever-changing requirements; and invest in transforming their people and processes to truly embrace an AI-first mindset.

After all, it is hard to keep pace with AI innovations that are nearing escape velocity, like Multi-modal, Neuro-Symbolic, Quantum, and Self-Improving or Evolutionary AI capabilities. Understanding where AI is headed is an essential factor when building, operationalizing, and governing your AI strategy.

RETHINKING RESILIENCE AND SECURITY

Finally, we cannot discuss the disruptive and transformative impact of AI without considering the escalating risk to an organization's security, resilience, and long-term sustainability. Like all groundbreaking technologies, AI systems introduce new gaps, risks, threat vectors, and variables that could make you more susceptible and compromise your integrity, confidentiality, and availability.

Concerns are high that AI can increase vulnerabilities to existing threats in 2025 [4]



4 GetApp, Four Steps to Get Ahead of AI-Enhanced Cyberattacks, IT Pros top Worry in 2025, Sep 23, 2024.

A recent report by Zscaler highlights a 595% increase in enterprise AI/ML transactions between April 2023 and January 2024, underscoring AI's growing integration into business operations. Concurrently, 18.5% of these AI transactions were blocked due to security concerns, reflecting the escalating threat landscape.[5]

Threat actors are employing advanced techniques such as adversarial attacks, where AI models are deceived by manipulated inputs, and data poisoning, which involves corrupting training datasets to alter AI behavior.

Additionally, model theft poses significant risks to intellectual property, while bias and fairness issues can lead to discriminatory practices, eroding stakeholder trust. The supply chain also presents vulnerabilities, with malicious actors exploiting third-party components to introduce backdoors into AI systems.

To navigate these challenges, organizations must adopt a proactive and structured approach to bolster AI security and resilience:

1. **Prioritize AI security at the leadership level.**
   Establish a dedicated AI Security Council comprising leaders from security, AI/ML, risk management, and compliance to oversee the development, governance, and enforcement of AI security policies.
2. **Integrate security into the AI development lifecycle.**
   Rather than a reactive, security-by-design philosophy, embed adversarial testing, bias mitigation, and compliance verification throughout the AI development pipeline for robust defenses against potential threats.
3. **Cultivate a security-first organizational culture.**
   Invest in comprehensive training programs that equip AI engineers and data scientists with the latest security best practices and promote a culture of "Responsible AI by Design" that encourages teams to anticipate and proactively mitigate vulnerabilities.
4. **Stay ahead of regulatory requirements.**
   Align AI security strategies with emerging global standards and regulations, such as the EU AI Act, NIST AI Risk Management Framework, and ISO 42001. Proactive compliance not only mitigates legal risks but also enhances organizational credibility.
5. **Develop AI-specific incident response protocols.**
   Traditional cybersecurity responses may not suffice for AI-related incidents. Formulate AI-centric security playbooks, establish AI Red Teams to simulate attacks, and implement automated rollback mechanisms to swiftly address and recover from adversarial events.

COMMVAULT ENABLES RESILIENCE IN THE EVER-EVOLVING WORLD OF AI

A traditional approach to **data protection** cannot stand up to the complexity of today's AI-first reality.

To be successful, organizations must embrace a cyber resilience platform that supports the depth of its AI data systems and the breadth of these new workloads. It should proactively scan for anomalies; remediate threats; and help you get back to business faster through better planning, testing, and recovery capabilities.

5 Zscaler, ThreatLabz 2024 AI Security Report, 2024.

Fortunately, at Commvault we are actively thinking through these challenges and can address these challenges in three ways:

1 **End-to-end AI data protection and recovery at scale**
AI workloads demand massive-scale data protection. Commvault provides fast recovery across on-prem, cloud, and hybrid environments, so AI systems remain operational even after disruptions.

Our platform is built to handle complex AI pipelines, offering fast, automated restoration of models, datasets, and metadata with minimal downtime. Whether dealing with petabytes of AI training data or real-time inference models, Commvault enables enterprises to restore at speed and scale.

2 **AI-driven cyber resilience and clean recovery**
AI security threats require proactive detection and clean recovery capabilities. Commvault leverages AI-powered anomaly detection to identify risks in real time, scanning for data manipulation, unauthorized access, and adversarial inputs before they cause damage. In the event of a compromise, Commvault enables recovery in a secure, isolated cleanroom, where organizations can validate, test, and analyze data integrity before restoration – so AI models and data sources remain uncompromised.

3 **Deep integrations for a unified security posture**
A fragmented security approach won't protect AI workloads. Commvault integrates with leading cybersecurity and AI platforms – including CrowdStrike, Microsoft, and Palo Alto Networks – to enhance threat detection, zero-trust security, and automated recovery. These integrations allow organizations to strengthen their overall security posture while maintaining visibility and control across their AI ecosystems.

AI-driven threats are evolving, but with the right strategy, organizations can stay ahead. A proactive approach – combining careful planning, AI-powered cyber resilience, and intelligent recovery – enables organizations to anticipate risks, neutralize threats, and restore operations. By integrating clean recovery, real-time threat detection, and deep security measures, enterprises can minimize risk resilience challenges and maintain control, so AI remains a driver of innovation, not vulnerability.

ALIGNING YOUR BUSINESS, AI, AND RESILIENCE STRATEGIES

AI has significant potential, but its effectiveness relies on strategic planning from the beginning, incorporating built-in security and resilience by design. As AI advances, so do the risks of adversarial attacks, data poisoning, and system failures that pose significant threats to continued innovation.

To be resilient, your organization must have strong leadership to bake security into AI development, train teams to spot risks, and stay ahead of regulations. Resilience requires clear response plans for AI-specific threats, including re-thinking your cyber recovery and resilience posture.

A proactive approach means AI remains secure, reliable, and ready for the future. After all, the question isn't whether AI will transform your business – it's whether you're building the resilience to withstand what comes next.