NUTANIX

How to Strengthen Security and Simplify Data Management with GenAI

Introduction

With cybercrime continuing to rise, security use cases remain a top priority among enterprises. As a result, cybersecurity teams are giving serious consideration to leveraging GenAI models to proactively detect and respond faster to potential threat behaviors.

Today's most common AI-enabled security use cases include:

- **Fraud detection.** Analyze historical transaction data to create AI models that can identify anomalies in transaction patterns and accurately detect attempts at fraud.
- **Threat detection.** Leverage AI to analyze vast amounts of data and identify patterns in areas like anomaly detection, threat intelligence and vulnerability assessment.
- **Alert enrichment.** Use AI to automatically gather and analyze context for security alerts so you can set priorities, reduce false positives and speed-up incident response.
- **Automatic policy creation.** Dynamically generate and update security policies based on ongoing analysis of the environment, threat landscape and industry best practices.

Considerations

AI capabilities that satisfy these use cases are now being included in the latest security and data protection tools.

Use cases like fraud detection can involve acquiring or creating customized AI models. Consequently, this will require cybersecurity teams to apply greater effort through significant AI experimentation, regular training of AI models and fine-tuning.

GenAI currently plays an adjunct role in most security use cases. For example, GenAI is often used to create synthetic examples of fraudulent transactions to increase the signal in training datasets used for fraud detection models.

For fraud detection and other internally developed security software, you'll also need an infrastructure that supports:

- Inference for AI models.
- Training and fine-tuning of AI models using company data.

Additionally, commercial security software that runs on-premises may have specific infrastructure requirements you will need to satisfy while SaaS solutions may have specific bandwidth requirements.

Because of the amount of data involved, security use cases can increase data storage needs and data management complexity.

Challenges

As you carefully identify your security use cases, expect to encounter these challenges:

- **Hybrid multicloud.** You will need to deploy AI-enabled security software everywhere you operate.
- **Specialized hardware.** This is required to accelerate inference – GPUs from NVIDIA or CPUs optimized for inference – and GPUs to support the training of AI models.
- **Containers.** Containers and Kubernetes are generally preferred to run and scale AI models and ensure high availability and efficient resource utilization.

You should also expect to encounter significantly greater data management challenges. Many organizations lack the skills and knowledge that's necessary to manage AI models and datasets throughout the AI lifecycle.

How Nutanix helps

Nutanix helps you deliver AI security tools that proactively safeguard your business. With Nutanix, you can accelerate AI-driven security initiatives across hybrid multicloud environments while simplifying data management.

Complete data services

Security use cases are data intensive. Your ability to move and manage data efficiently between the datacenter, cloud and the edge can be critical when it comes to real-time threat detection.

Nutanix eliminates data management challenges with software-defined data services that simplify storage operations across the datacenter, cloud and edge.

Nutanix combines the data services you need with the enterprise-class capabilities you expect. We eliminate the need for separate file, block and object storage systems while reducing cost and complexity.

A hardened platform

With Nutanix, security begins with a robust software foundation built for hybrid multicloud architectures. Nutanix starts with a hardened software platform for hyperconverged infrastructure and builds on that foundation.

Our capabilities strengthen your security posture by enabling you to detect and respond quickly to threats that can lead to data loss and business disruption. You can count on Nutanix to provide a secure foundation for AI and other critical workloads.

Additional guidance

For more guidance, download the recently published eBook, The Essential Guide to Navigating AI and Cloud-Native Deployments. This indispensable guide explains what you need to build and deploy AI models that strengthen security while dramatically simplifying data management and AI model containerization.

NUTANIX

info@nutanix.com | www.nutanix.com | @nutanix

©2025 Nutanix, Inc. All rights reserved. Nutanix, the Nutanix logo and all product and service names mentioned herein are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. All other brand names mentioned herein are for identification purposes only and may be the trademarks of their respective holder(s).

GC-AI-HowToStrengthenSecurityandSimplifyDataMgmtwithGenAI-Infobrief-FY25Q2-v3 03262025