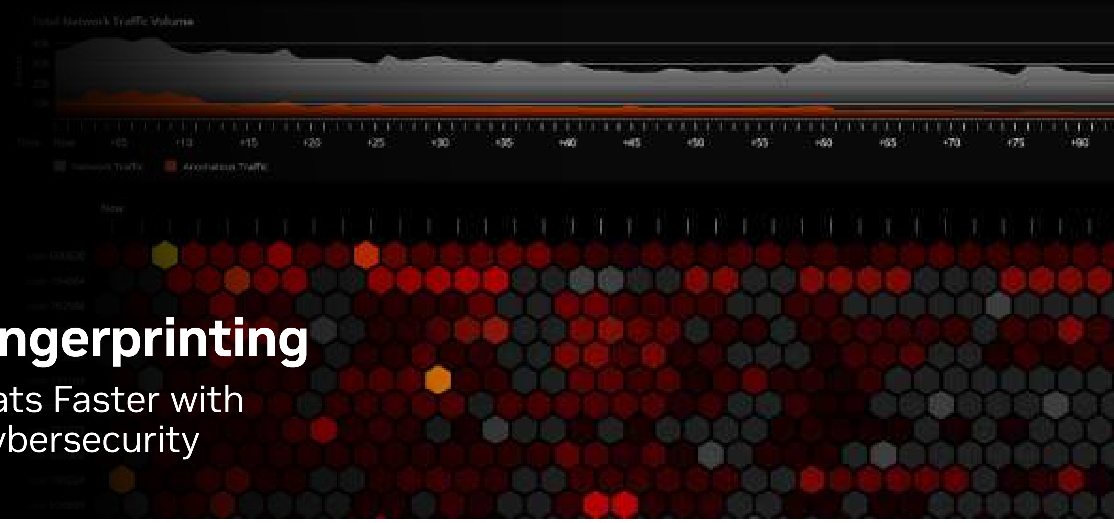
SOLUTION BRIEF



NVIDIA Digital Fingerprinting

Identify and Act on Threats Faster with
Morpheus AI-Powered Cybersecurity

Cybersecurity Is a Data Problem

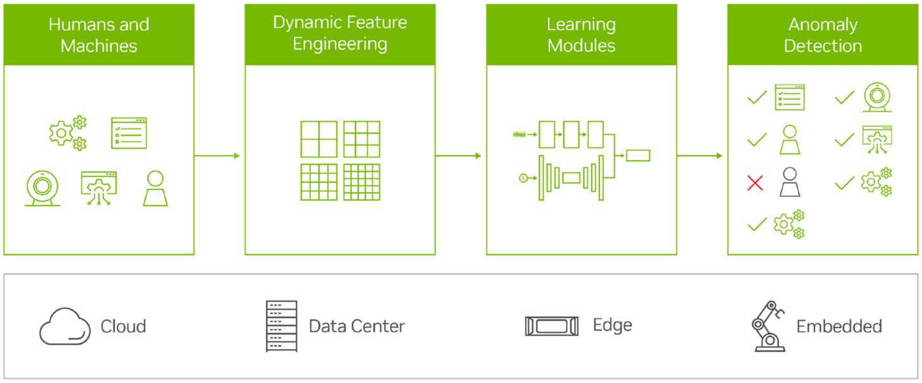
Network traffic continues to increase - the number of internet users across the globe reached 5 billion in 2022 and continues to rise. As the number of users expands, so does the number of connected devices, which is expected to grow into the trillions. The ever-increasing number of connected users and devices leads to an overwhelming amount of data generated across the network. According to IDC, data is growing exponentially every year,[1] and it's projected the world will have generated 179.6 zettabytes of data by 2025. This equates to an average of 493 exabytes of data generated per day.

All of this data and network traffic poses a cybersecurity challenge. Enterprises are generating more data than they can collect and analyze, and the vast majority of the data coming in goes untapped. Without tapping into this data, an enterprise can't build robust and rich models to detect abnormal deviations in their environment. The inability to examine this data leads to undetected security breaches, long remediation times, and ultimately huge financial losses for the company being breached. With cyberattack attempts per week rising by an alarming 50 percent in 2021[2], cybersecurity teams must find ways to better protect these vast networks, data, and devices.

AI Is Critical to Addressing Cybersecurity Challenges

NVIDIA Morpheus is a cloud-native application framework that enables cybersecurity developers to create optimized AI pipelines for filtering, processing, and classifying large volumes of real-time data. Bringing a new level of information security to the data center, cloud, and edge, Morpheus uses AI to identify, capture, and act on threats and anomalies that were previously impossible to detect.

NVIDIA Morpheus enables many cybersecurity workflows. Its prebuilt, end-to-end workflow for digital fingerprinting is designed to analyze the behavior of every human and machine across the network to detect anomalous behavior. With Morpheus, you can implement unsupervised learning to do this on a scale previously impossible.



Key Challenges

- > Credential attacks are the most common entry point.
  - > On average, a breach costs $4.5 million.
  - > It takes ~243 days to identify a breach and another 84 days to contain it.[3]
- > Compromised credentials can be used to infiltrate targeted systems, applications, and accounts.
- > Exposed credentials lead to increased attacks.
  - > Of organizations hit by credential attacks, 95 percent observed up to 3.3 billion malicious login attempts over the course of a year.[4]

[1] IDC, Worldwide IDC Global DataSphere Forecast, 2022-2026: Enterprise Organizations Driving Most of the Data Growth, IDC #US49018922, May 2022

[2] DARKReading

[3] IBM Security, 2022

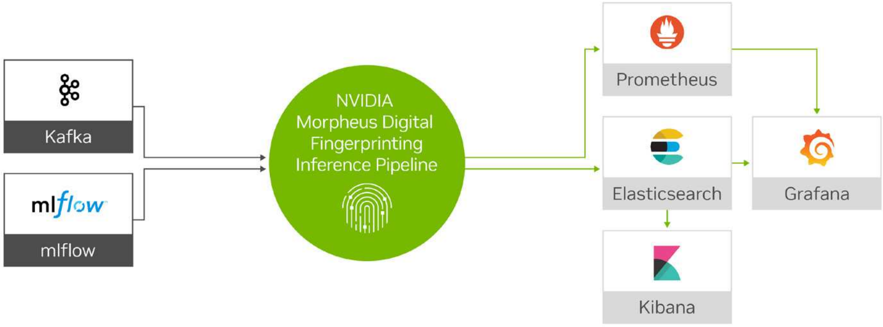
[4] Verizon Data Breach Investigations Report 2021

Digital Fingerprinting AI Workflow

NVIDIA Morpheus digital fingerprinting flags when user and machine activity patterns shift. The Morpheus digital fingerprinting example workflow provides tangible ways to start instantiating digital fingerprinting with the Morpheus SDK. The digital fingerprinting reference workflow includes both training and inferencing pipelines. The following cloud-native Kubernetes services are used with this workflow:

- Kafka
- MLflow
- Prometheus
- Elasticsearch
- Kibana
- Grafana
- S3 Compatible Object Storage

The Morpheus digital fingerprinting reference workflow includes a Kafka producer with a sample dataset and web server, as well as Python code and a custom debugger to allow debugging anywhere within the pipeline. The digital fingerprinting reference workflow is a starting point, and the components included are optional and interchangeable. Additionally, options are available for developing and running the pipelines in the cloud or on premises.



Benefits of NVIDIA Morpheus digital fingerprinting

- Provides 100 percent data visibility and uniquely fingerprints every user, service, account, and machine
- Includes intelligent alerts with actionable information
- Enables cybersecurity analysts to identify, capture, and act on threats faster with visualization
- Reduces hundreds of millions of events per week to 8–10 potentially actionable insights daily
- Cuts the time to detect from weeks to minutes, for certain attack patterns

Get Started with Morpheus Digital Fingerprinting

Try NVIDIA Morpheus for free on NVIDIA LaunchPad. NVIDIA LaunchPad provides enterprises and organizations around the globe with immediate, short-term access to the NVIDIA Morpheus AI framework, including the digital fingerprinting prebuilt model, running on private accelerated computing infrastructure, to test and prototype AI cybersecurity workflows.

Learn More

To learn more about NVIDIA Mopheus visit:

nvidia.com/morpheus

© 2022 NVIDIA Corporation. All rights reserved. NVIDIA, the NVIDIA logo, and CUDA are registered trademarks and/or trademarks of NVIDIA Corporation in the United States and other countries. Other company and product names may be trademarks of the respective companies with which they are associated. NOV22

FPO