AI Stack

Network Visibility for AI / ML Applications

Generative AI (genAI) is increasingly being integrated into business operations, offering opportunities for efficiency and value creation. However, it also presents risks related to data security, privacy, and compliance.

Businesses aim to strike a balance between leveraging genAI's benefits and enforcing stringent security measures. According to a 2023 IBM report, **82% of businesses** see AI-related risks as a top priority, and **45% of data breaches** are now AI-driven in some form. Moreover, compliance costs for companies using AI tools have surged by **30%** due to evolving regulations.

To mitigate risks, organizations must implement clear guidelines and protective measures, ensuring that genAI is used responsibly while maintaining robust data protection and compliance standards.

Highlights

- **Monitor Use And Reach Of AI** – Monitor critical network segments with unauthorized use of AI or use of AI in unintended domains.
- **Leverage Deep Packet Inspection (DPI)** – Ensure detailed data analysis for detecting and filtering GenAI applications.
- **Enhance Detection Across Traffic Types** – Apply filtering to both encrypted and cleartext traffic, with advanced options for cleartext.
- **Implement Decryption Capabilities** – Gain visibility into GenAI application layers, crucial for analyzing encrypted traffic.
- **Use Session-Aware Detection** – Gain better accuracy over traditional packet-based filtering.
- **Perform Deep Packet Inspection (DPI)** – Analyze multiple protocol headers and payloads, including encrypted traffic (SSL, TLS, QUIC).
- **Leverage Application Signatures** – Enable high-performance real-time detection and filtering.
- **Utilize Dynamic & Static Signatures** – Apply both for flexible filtering and metadata generation.

KEYSIGHT

Knowing whether AI, particularly generative AI (genAI), is being used in a corporate setting is crucial for several reasons:

1. **Data Security & Privacy Risks** – AI models often process large amounts of sensitive data. If not properly controlled, they can expose confidential business information, customer data, or trade secrets. Studies show that over 60% of companies cite data security as their top concern when adopting AI.
2. **Regulatory Compliance** – Many industries operate under strict data protection laws, such as GDPR (General Data Protection Regulation) in Europe or CCPA (California Consumer Privacy Act). Failure to ensure AI compliance can result in significant fines—GDPR penalties alone have exceeded $4.3 billion USD since its implementation.
3. **Bias & Ethical Concerns** – AI systems can inadvertently introduce biases into decision-making processes, leading to discrimination in areas like hiring, lending, and customer service. Research shows that AI-driven hiring tools can have up to a 30% higher bias rate if not properly monitored.
4. **Intellectual Property Risks** – AI-generated content can create copyright and ownership issues. Companies must be aware of whether their AI tools are using proprietary data or infringing on third-party intellectual property.
5. **Operational Transparency & Trust** – Employees, customers, and stakeholders need to understand when AI is being used to ensure trust and accountability. Surveys indicate that 75% of consumers prefer transparency about AI involvement in decision-making when interacting with businesses.

How do security operations teams "see" if genAI is being used, where, for what, and if its use is not nefarious?

Keysight Vision Packet Brokers with AI Stack enable visibility into AI usage, businesses can mitigate risks, build trust, and ensure AI is used responsibly while maximizing its benefits.

Solution

Comprehensive visibility into genAI applications requires access to network traffic for detection, filtering and inspection.

1. **Seeing the Content of AI Applications, Incredible Detailed View of Privacy/Data**

   For genAI applications running over SSL/TLS (HTTPS), the payload can be decrypted using either Keysight SecureStack or any external SSL/TLS decryption solution available. GenAI applications transported over QUIC can be inspected using header-based DPI in Keysight AppStack; however, their payload cannot be decrypted currently, but there are network security workarounds for enforcing the clients to use TLS instead of QUIC (see the documentation from your network firewall or proxy/gateway vendor).

- **Deep Packet Inspection (DPI) & GenAI Detection**
  - The effectiveness of detecting and filtering GenAI applications depends on how much detailed data the DPI engine can access.
  - Detection works on both encrypted and cleartext traffic, but cleartext allows for deeper filtering and analysis.
  - Since 90%+ of internet traffic (and nearly all GenAI traffic) is encrypted, decryption is essential for inspecting the application layer.

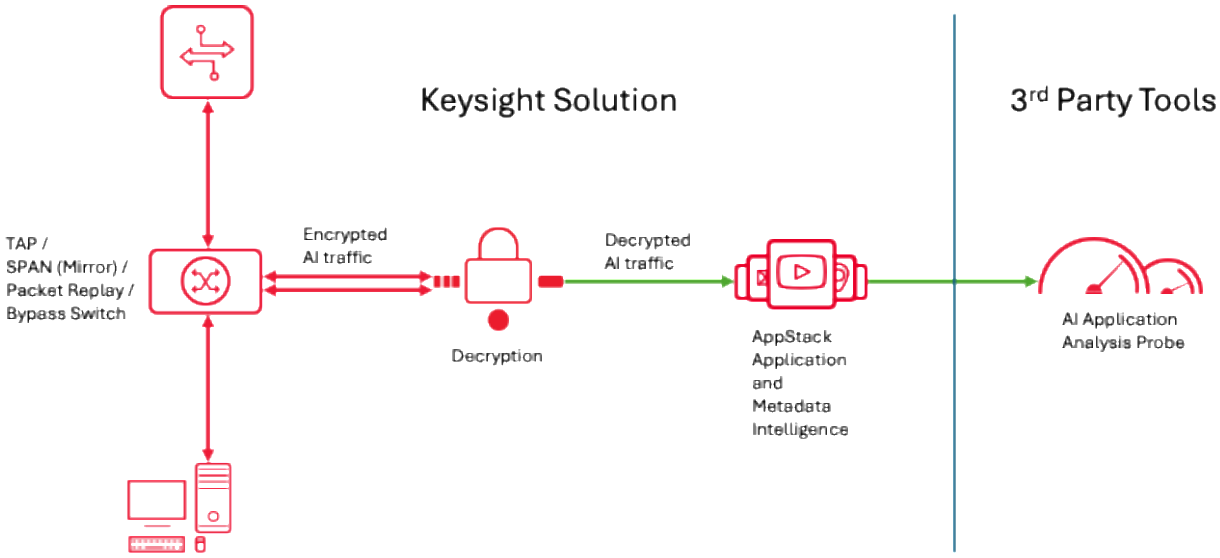
- **Decryption for GenAI Applications**
  - SSL/TLS (HTTPS) traffic can be decrypted using Keysight SecureStack or other SSL/TLS decryption solutions.
  - QUIC-based GenAI traffic encrypted headers can be inspected by Keysight AppStack. The payloads cannot currently be decrypted, but network security measures can enforce TLS usage instead (check firewall/proxy documentation).

- **Key Benefits of Decrypting GenAI Traffic**
  - Access to detailed insights: AI model versions, usernames, actions, and configurations become visible.
  - AI prompts & responses can be searched and analyzed for user behavior, malicious code detection, or data leakage.
  - AI-generated media content (images, sound, video) can be extracted and analyzed using specialized tools.
  - User-uploaded or AI-generated files can be retrieved for security inspection and compliance checks.
  - Advanced DPI filters allow fine-tuned detection of GenAI components (e.g., client type, actions like search/share/feedback).
  - Layer 7 protocol data (e.g., HTTP headers, device type, OS details) enhances filtering accuracy and can be exported for AI/ML analysis, reporting, and long-term retention.

Since more than 90% of internet traffic (and almost 100% of genAI application traffic) is encrypted, the ability to see inside the contents of the genAI application layer requires decryption capabilities.

For genAI applications running over SSL/TLS (HTTPS), the payload can be decrypted using either Keysight SecureStack or any external SSL/TLS decryption solution available.

GenAI traffic decrypted by SecureStack or third-party appliances can be fed into AppStack through the following flow:



2. Detecting and Filtering AI Application Traffic

Detecting AI applications through network traffic analysis requires identifying distinct patterns, protocols, and behaviors associated with AI workloads.

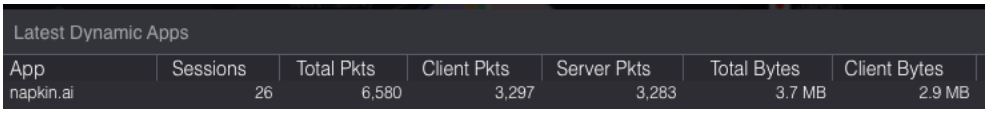
- Keysight AppStack advantages:
  - Uses a session-aware engine by default, which has advantages over packet-oriented detection and filtering engines. AppStack can track the entire application flow simply by matching a single packet belonging to that application flow. With buffering support, the full application flow, from handshake to finish, can be filtered and forwarded, even if the match is found later in the flow after the initial handshake.
  - Performs DPI in a wide range of protocol headers and payloads: TCP, UDP, SCTP, SSL, TLS 1.0-1.3, QUIC and all the Layer 7 applications. AppStack can detect genAI applications transported over any of these protocols, even the ones using encrypted QUIC headers.

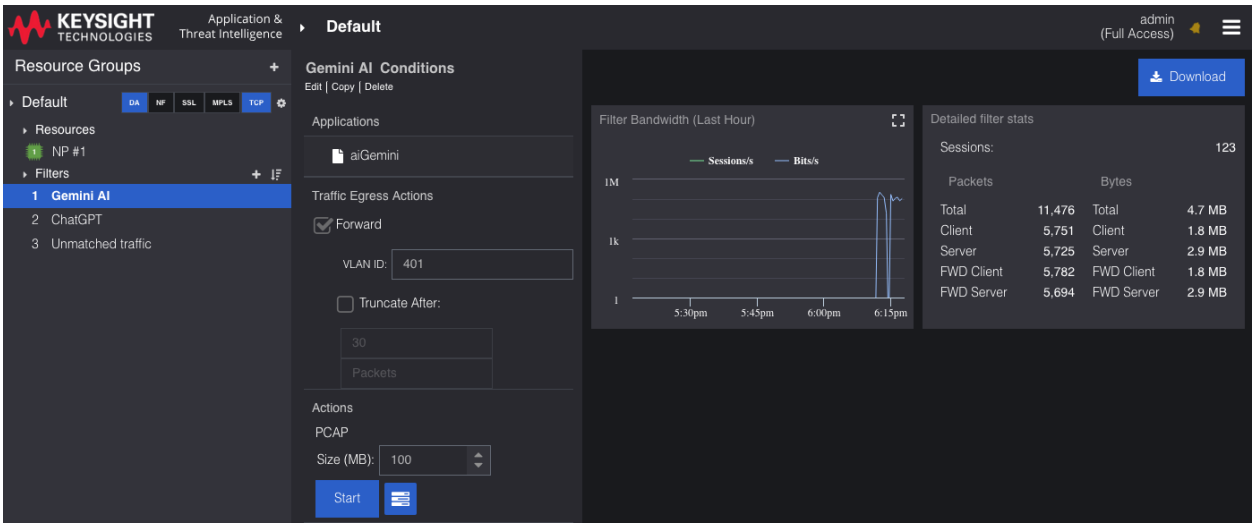
The following techniques, available in Keysight AppStack, can be used:

- Signature-based detection and filtering

  AppStack leverages the power of application signatures to deliver high performance real-time detection and filtering of network traffic generated by distinct applications. There are three signature types supported by AppStack:

  - **Static signatures:** Pre-defined, always available and regularly updated on a subscription base.
  - **Dynamic signatures:** AppStack detects new patterns at OSI Layers 4-7 in traffic flows that have not been matched by existing static signatures and identifies these patterns as new dynamic signatures. Dynamic signatures can be used in filters and metadata generation just like static signatures.
  - **Custom signatures:** These can be manually created and added to AppStack, for identifying specific applications by accurately pinpointing the exact field(s) and value(s) to match. For advanced users, custom signatures offer the highest level of control in the application detection process. Dynamic signatures can also be converted to custom signatures.

Signature type	genAI filtering examples
Static	AppStack has released several signatures for genAI applications: • OpenAI • ChatGPT • Beautiful.ai • Character.ai • Apple Siri
Dynamic	AppStack detects genAI applications without signatures as Dynamic Apps. Here is an example for napkin.ai: 
Custom	For highest accuracy, Custom Apps for genAI applications can be created, either starting from an existing Dynamic App, or writing the signature from scratch or from templates. Here is an example from a section of a custom signature, which can detect the Gemini app by matching the Server Name Indication (SNI) in the TLS handshake: <signature uuid="cus-77066151-43bc-4a16-9552-c22768ce794b" idapp="true"> <inspect field="ssl_ext_sni"> <value lanchor="true" ranchor="true">gemini.google.com</value> </inspect> </signature>



Use of a Custom Signature to filter and forward Google Gemini AI

- Regular Expressions (RegEx)

  Taking advantage of the session-aware engine, AppStack supports genAI application detection by matching RegEx against network traffic. RegEx needs to match a single value in a single packet of the genAI application flow, for the entire application flow to be matched, filtered and forwarded. There is no need for the RegEx to match multiple fields or multiple packets of the same application flow.

  For example, this is a simple RegEx filter which can be used for the Google Gemini app:

Regex
gemini\.google\.com

  More advanced RegEx filters can be used for matching more complex application flows.

3. Deep Analytics of AI Use and AI Used in Cybersecurity Applications

- AI usage in cybersecurity can be deeply analyzed using advanced monitoring tools such as probes and sensors. These tools can track and reconstruct interactions within GenAI applications, even if they are encrypted. They analyze user prompts, AI-generated responses, and other inputs, including uploaded documents, audio, and video exchanges.
- By leveraging such deep analytics, cybersecurity systems can gain a comprehensive understanding of how AI is being used across an organization or network. This capability allows for the detection of unauthorized, inadvertent, or malicious AI usage that could lead to data breaches, intellectual property theft, or security vulnerabilities. Additionally, these monitoring tools can help enforce compliance policies, ensuring that AI technologies are used responsibly and within regulatory frameworks.
- Cybersecurity applications can take proactive measures to mitigate risks, such as blocking unauthorized AI interactions, flagging suspicious activities, and preventing the leakage of sensitive or confidential information. This level of AI monitoring plays a crucial role in strengthening overall cybersecurity defenses and safeguarding digital assets from exploitation.

Leading 3rd party cybersecurity platform suppliers which enable seamless AI monitoring solutions include (non-exhaustive).

- **Network Detection and Response:** uses AI and machine learning to monitor network traffic for threats, detect anomalies, and respond to potential cyberattacks in real time.
- **Threat Detection & Prevention:** AI-driven systems analyze network traffic and user behavior to identify anomalies and potential cyber threats such as malware, ransomware.
- **Security Information and Event Management (SIEM):** AI helps process and analyze vast amounts of security data to detect and prioritize threats including automated correlation of logs and alerts.
- **Deception Technology:** AI-driven deception techniques create decoys and traps to mislead attackers and gather intelligence, including fake assets or credentials to lure cybercriminals.

Ordering Information

AI Stack features are available on Vision ONE, Vision X and Vision 400 by applying the following licenses on top of the base unit, hardware modules and port licenses:

Description	Vision 400 part number
AppStack Application Intelligence (select one)	LIC-V400-AS-SSAS, SUB-V400-AS-SSAS, LIC-V400-AS-APFL or SUB-V400-AS-APFL
AppStack Signature Updates (optional)	SUB-V400-AS-APTL
Inline (required if Inline Decryption is selected; select one)	LIC-V400-INLN or SUB-V400-INLN
Inline Decryption (optional) + Host Categorization (optional)	LIC-V400-SS-INLD SUB-V400-SS-HCS

Description	Vision X part number
AppStack Application Intelligence (select one)	LIC-VX-SSAS, SUB-VX-SSAS, LIC-VX-APFL or SUB-VX-APFL
AppStack Signature Updates (optional)	SUB-VX-APTL
Inline (required if Inline Decryption is selected)	LIC-V400-INLN
Inline Decryption (optional) + Host Categorization (optional)	LIC-VX-ASSL SUB-VX-ASSL-HCS
Out of Band Decryption (optional; select one)	LIC-VX-PSSL or SUB-VX-PSSL

Description	Vision ONE part number
Visibility Application Module (not required if Inline Decryption is selected)	MV1-VAM
AppStack Application Intelligence (select one)	LIC-V1-APPS2 or SUB-V1-SSAS
AppStack Signature Updates (optional)	SUB-V1-APTL2
Inline (required if Inline Decryption is selected)	LIC-V1-INLN
Inline Decryption bundled with Visibility Application Module (optional; select one)	MV1-ASSL-1G, MV1-ASSL-2G, MV1-ASSL-4G, MV1-ASSL-10G
Host Categorization for Inline Decryption (optional; select one)	SUB-ASSL-HCS-1G SUB-ASSL-HCS-2G SUB-ASSL-HCS-4G SUB-ASSL-HCS-10G
Out of Band Decryption (optional; select one)	LIC-V1-PSSL or SUB-V1-PSSL

Support

Keysight's Visibility products are backed by our industry-leading expertise. Our comprehensive product support does more than ensure uptime – it ensures a competitive edge. The Keysight support team partners with customers to:

- Avoid downtime and keep schedules on track
- Implement according to industry specifications
- Develop best practices to meet individual needs and objectives
- Maximize efficiency and reduce operating expenses
- Protect and maximize investments in test and visibility

In addition to the above, Keysight customers registering for the secure area and access to the Support Site will also be able to view and download our product Security Advisories.

Access Keysight Visibility Support

About Keysight Visibility

Connect and secure the world with dynamic network intelligence

The need for always-on networks is pervasive, and expectations are high when it comes to keeping them connected and secure. As technologies advance, edge computing, cloud environments, sophisticated security breaches, increasing bandwidth requirements, and demanding compliance regulations make it challenging to extract actionable insight from your network.

Keysight can help. Customers rely on our solutions to deliver rich data about network traffic, applications, and users across any networking environment. This deep insight is what we call dynamic network intelligence. It helps you continuously innovate, meet aggressive service level agreements, and keep applications running smoothly and securely.

Learn more about Keysight Visibility Solutions