**Eric Somogyi**
**5/11/2025**
**NET 577 - Final Research Paper**

# Artificial intelligence and its advantages disadvantages for network configuration, management, IDS/IPS, ZTA, SD-WAN, automation, SIEM, and SASE technologies

# Table of Contents

**Abstract**

This research paper is about the developments in the cloud architecture and public cloud industry that businesses and governments use to operate, with recent developments in applications integrating machine learning models and artificial general intelligence to enhance the overall security posture of organizations. With the complexity of the architectures slightly changing in the virtual cloud environments, and more enhanced escalated cyber threats, this paper explores the advantages and disadvantages of software where some form of AI is used in transforming network security intrusion detection and prevention systems IDS/IPS, threat detection on edge networks,

This paper will also explore and examine the many features and qualities of AI in the zero trust architecture (ZTA), secure access service edge (SASE) AI technologies, network configuration automation with machine learning techniques and NGFW, AI governance tools, and how the industry from a software/hardware engineer perspective is currently expected, and how these same open source technologies can be used in automation technology to defend against cyber threats in specific AI technologies in modern global networks.

**Introduction**

Cloud computing became a foundational technology over a decade ago (need to insert fact quote here for refence with exact percentage from source) for businesses and governments, driving operational efficiency, scalability, and innovation through cloud services. As cloud architectures evolve to meet these demands, their complexity has increased, introducing new security challenges in virtualized environments. The cyber attack surface has widened (need to insert face source example here to prove my argument), and with cyber threats growing more complicated organizations face ever changing new security challenges in cloud environments, which pose a risk to organizational data and infrastructure. The integration of AI and using ML foundation models with a combination of databases, for real time analytics (need to fix what I mean here), and early forms of artificial general intelligence, has contributing to the evolving landscape of how virtual portal allow engineers to program secure public and private cloud networks. This research paper investigates advantages and disadvantages of AI applications and open-source machine learning technologies that revolutionize network security, focusing on technologies such as intrusion detection and prevention systems (IDS/IPS), threat detection on edge networks, zero trust architecture (ZTA), and secure access service edge (SASE). It also discusses how ML techniques enables network configuration automation and complements SASE services.

## Review of Literature

In this section, I analyze various cybersecurity services, frameworks, and network systems complemented with studies from various technical papers and industry reports on the application of AI) in enhancing cybersecurity across five key domains: network configuration and management and next generation firewalls, intrusion detection and prevention systems (IDS/IPS), secure access service edge (SASE), zero trust architecture (ZTA), and public cloud security. The review explores both the advantages and disadvantages of AI integration.

### Network Configuration and Management and Next Generation Firewalls

Since most companies will be using cloud services by 2025, there are many procedures and guidelines to follow in network configuration and management. Organizations are configuring their networks through next-generation firewalls (NGFW) in on-premise, hybrid, and public cloud deployments, and these firewalls have advanced networking capabilities such as advanced networking, threat inspection and detection, web filtering, internet of things (IoT) security, network sandboxing, zero trust network access (ZTNA), operational technology (OT) security, domain name system (DNS) security, software-defined wire-area (SD-WAN) network capabilities, and advanced logging and reporting capabilities. Some of these capabilities from the firewall are designed to use multiple vendor specific or 3rd party AI/ML security services to stop advanced threats and prevent business disruptions (paraphrased from techblog). The main disadvantage with these new technologies, is the complexity and personnel skill it takes to program the hardware correctly, and there is increased cost to using them, but it does contribute to the zero trust network access model of securing resources and network for the long term to decrease the attack surface.

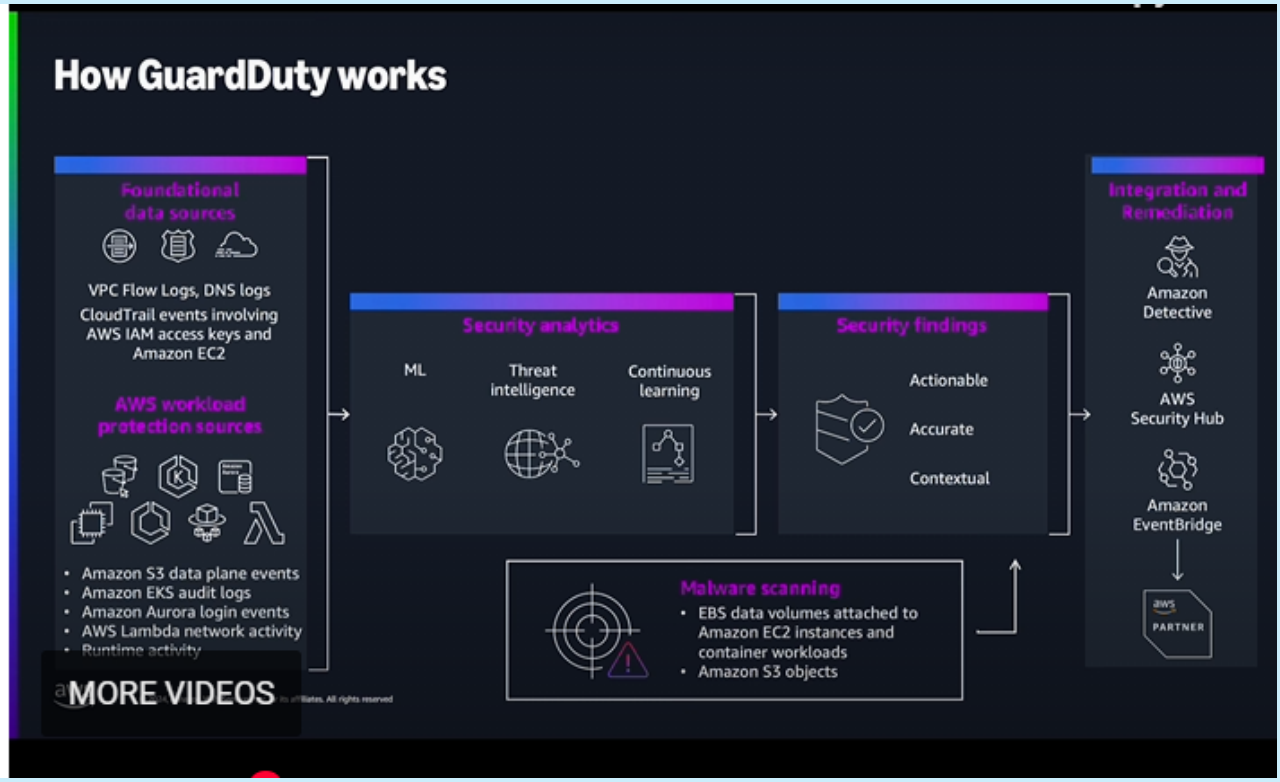
According to Palo Alto networks, 2008 was when was the 3rd generation next generation firewalls (NGFW) came out. As of 2010 through 2020, 4th generation ML-powered next-generation firewalls came out. The difference between them are the 4th generation firewalls were able to focus on advanced threat prevention, SSL/TLS decryption, leverage automation for policy management and threat response with security orchestration tools, emphasis on a zero-trust architecture of continuous verification. Additionally, the 4th gen NGFW's introduced in 2020, use in line machine learning prevention to deliver real time inline zero-day protection. This new advancement in firewall technology enable machine learning technology to analyze network traffic patterns to identify anomalies which the older generation of firewalls would not be able to successfully respond to with present day threats. These new ML-powered NGFW's also streamline security management allowing the security team to quickly adapt to updates and human error. Below is the Gartner Magic Quadrant from 2022, for NGFWs:


**AI Governance Tools**

For cybersecurity professionals, companies, and developers to protect against malicious threat actors targeting their large language models (LLMS), there is also new AI tools for AI governacne and observability. From the Zscaler 2024 ThreatLabz Report, “Malware threat actors are leveraging AI tools to scan networks for vulnerabilities, generate exploits tailored to specific configurations, and facilitate the rapid spread of ransomware within compromised environments” (ZTL2025). One way threat actors achieve this is by using Agentic AI, which is “Agentic AI is a type of AI that acts autonomously, making decisions, analyzing its environment, and adapting its actions to achieve specific goals—all with little to no human oversight. Key capabilities: Operates independently and adapts in real time, Makes decisions and takes actions, Executes complex, multistep tasks with minimal supervision, More advanced than chatbots or smart assistants, Can be leveraged for both innovation and cyberthreats “ (pg. 31 (ZTL2025). To combat this, there are several software technologies that exist in order to defend and protect against unauthorized changes. These software technologies are built with artificial intelligence scanning capabilities and advanced learning algorithms to protect against sophisticated attacked and are referred to as Agentic Detection Triage and Agentic Response. A few are NVIDIA Nemo Guardrails, Crowdstrike Charlotte AI, Amazon Bedrock Guardrails, Amazon Sagemaker Model Monitor, AWS Config, Microsoft Purview, Microsoft Defender for Cloud, Azure Policy, and ServiceNow AI Agent Orchestrator.

**Intrusion Detection and Prevention Systems (IDS/IPS)**

An intrusion detection system (IDS) is a passive system that scans traffic for threats and reports the data back to the administrator. An intrusion prevention system (IPS) enhances security through better visibility into attacks, increased efficiency in inspecting traffic, and less resources for managing vulnerabilities and patches. There are network-based intrusion prevention systems (NIPS), host intrusion prevention systems (HIPS), network behavior analysis (NBA), and wireless intrusion prevention systems (WIPS). In 2017, Amazon Web services launched Amazon GuardDuty, which is a cloud-based IDS that uses machine learning (ML) models to identify suspicious and malicious activity in an AWS cloud environment. AWS GuardDuty scans all instance environments and container workloads for malware detection. In the screenshot below, we can see how GuardDuty uses machine learning and reinforcement learning machine learning algorithms to continually learn and update its environment to detect threats. This is just one example of how artificial intelligence and machine learning has benefited IDS/IPS systems

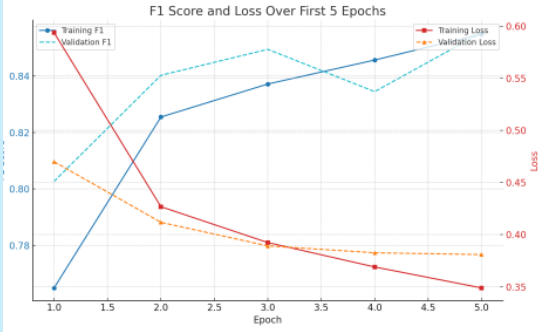



Next, provided in the “Anomaly Based Intrusion Detection using Large Language Models” IEEE study, this research “has demonstrated the vital importance of integrating diverse network and IoT datasets to enhance data quality and quantity for anomaly detection. Through effective data transformation and the application of Large Language Models (LLMs), we have successfully navigated the challenges posed by disparate dataset features. Our findings particularly highlight the benefits of this integration, with improved model performance across various attack categories. In the specific case of the UNSW-NB15 dataset, which initially had low occurrence rates in certain attack categories, extending the training to over 40 epochs significantly enhanced the accuracy for ’Backdoor’ and ’DoS’ attacks while reducing the overall loss” (pg 7

ABIDLLM). The UNSW-NB15 Dataset located here: https://research.unsw.edu.au/projects/unsw-nb15-dataset is a dataset that contains 9 types of attacks. According to this study, In the figure below from ABIDLLM, we can see how the performance of a machine learning model (the tokenizer called UNSW-NB15), had a near perfect F1 score and high accuracy 97% for Man in the Middle Attacks (MITM). Even though the model had high accuracy for Edge-Iot devices and could use improvement on varied datasets, it does prove that using ML techniques is necessary for identifying attacks across different network environments, which is an advantage of using ML/AI in cybersecurity practices.

the TON-IoT dataset.

- **UNSW-NB15**: As shown in Figure 2, the tokenizer trained on all datasets with a vocabulary size of 20,000 demonstrates significant improvements in both training and validation metrics over the first five epochs. The F1 score steadily increases, peaking at 0.8554 by epoch 5, while the validation loss decreases to 0.3809, indicating optimal model performance. Both training and validation F1 scores show clear progression, reflecting the model's ability to generalize effectively with a larger and more diverse vocabulary. The decrease in validation loss suggests that the model learns meaningful patterns and avoids overfitting during these early epochs. This highlights the importance of using a larger vocabulary size to capture complex network traffic patterns.
- **Edge-IIoT**: The model achieved near-perfect accuracy across all classes, with an F1 score of 0.99999 and a validation loss as low as 0.0000441 by the third epoch. Even for minority classes like Ransomware (97% accuracy) and MITM (99% accuracy), the model maintained strong performance, demonstrating its robustness in handling class imbalance. Despite potential concerns of overfitting due to the high accuracy and low validation loss, future work will test the generalizability of the fine-tuned model by applying it to other datasets to ensure its broader applicability. This approach will help confirm whether the model overfits to the EDGE-IIoT dataset or generalizes effectively to unseen data from different network environments.




ig. 2. Training and Validation F1 Scores and Loss Across Epochs on the

Furthermore, as noted in the "Implementing the NIST Zero Trust Architecture with Zscaler" paper, "the Zero Trust Exchange is not limited to the basic NIST ZTA framework; it offers zero trust protection not only for users, but also for workloads and Internet of Things (IoT) / Operational Technology (OT) environments" (pg. 4 ZTA2022). This is evidence that Zscaler has built a framework that utilizes similar infrastructure that supports filtering of traffic and workloads from IoT/Operation technology environments.

**Secure Access Service Edge (SASE)**

SASE leverages AI to integrate networking and security functions into a unified, cloud-native platform. AI algorithms analyze traffic, detect threats, and enforce policies across distributed environments. Machine learning models mitigate distributed denial-of-service (DDoS) attacks by identifying real-time traffic anomalies. The paper "Machine Learning and the Secure Access Service Edge" analyzes the necessity for Machine Learning (ML) to be included in the SASE framework. In the figure below, we can see there are several options where ML functions can be implemented in specific microservices to control and assist in administration of the SASE services, like Firewall as a Service (FWaaS), Cloud Access Security Broker (CASB), SD-WAN, or Secure Web Gateway (SWG).

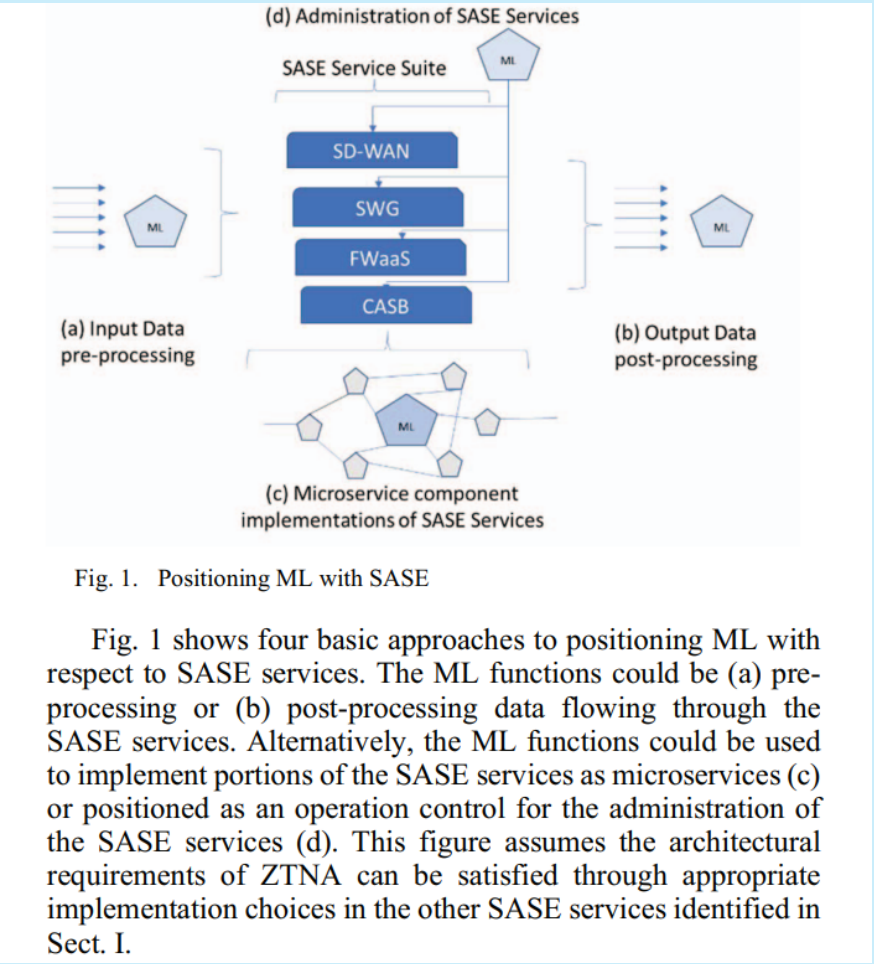



Fig. 1. Positioning ML with SASE

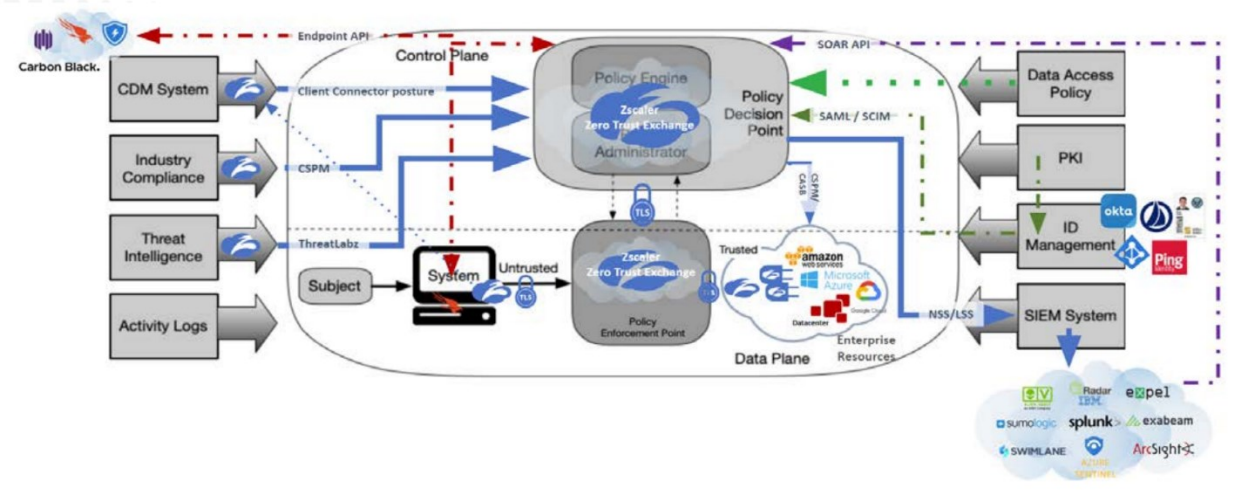
Fig. 1 shows four basic approaches to positioning ML with respect to SASE services. The ML functions could be (a) pre-processing or (b) post-processing data flowing through the SASE services. Alternatively, the ML functions could be used to implement portions of the SASE services as microservices (c) or positioned as an operation control for the administration of the SASE services (d). This figure assumes the architectural requirements of ZTNA can be satisfied through appropriate implementation choices in the other SASE services identified in Sect. I.

**Zero Trust Architecture (ZTA)**

Zero Trust Architecture (ZTA) is a security model that assumes no implicit trust within or outside the network perimeter, requiring continuous verification of users, devices, and applications (paraphrased definition). The U.S. Government decided in 2022 that by end of the fiscal year 2024, which orders the Federal Government agencies to meet cybersecurity standards and objectives by migrating to a zero-trust architecture strategy. The memorandum summarizes how federal applications cannot rely on network perimeter protections to guard against unauthorized

access. When comparing the requirements from this memo to the zero-trust architecture, there is beneficial tradeoffs to make the migration. When comparing the requirements to Jacob Serpa's Zscaler blog on the complexity of a zero-trust architecture, he explains how if companies continue to force-fit legacy security approaches in the cloud, cost and complexity will increase due to improper defenses for modern complex security needs. When an organization migrated to the zero trust cloud architecture, the enterprise does not have to maintain or purchase appliances, saving them costs in the cloud zero trust architecture model. Moving forward, the memorandum also references NIST 800-207 publication from 2020 for Zero Trust architecture, where this publication does establish that artificial intelligence and other software-based agents are being deployed to manage enterprise networks, but "the biggest risk when using automated technology for configuration and policy enforcement is the possibility of false positives (innocuous actions mistaken for attacks) and false negatives (attacks mistaken for normal activity) impacting the security posture of the enterprise." This can be a costly expense to many organizations to manage.

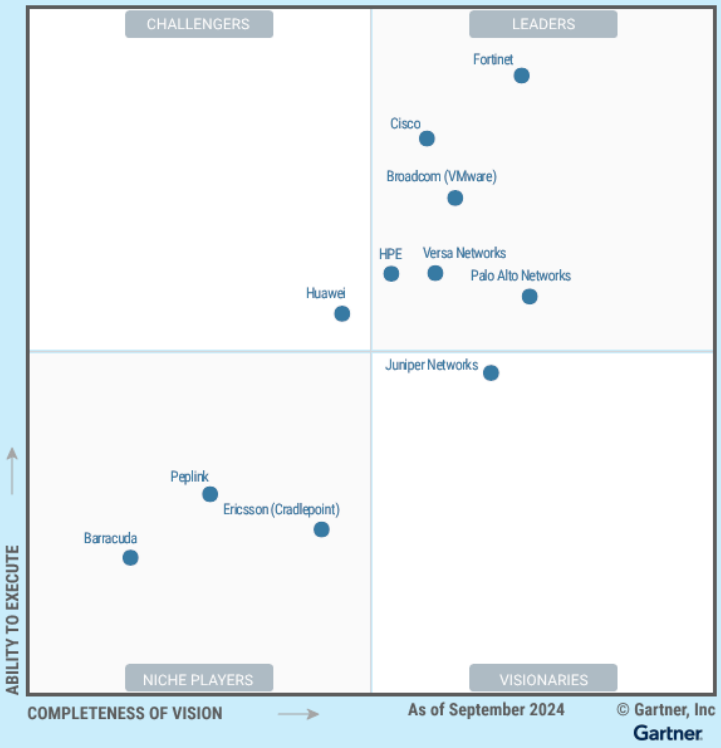
Next, this data point displays that the Zscaler ThreatLabz 2025 AI Security Report (ZTL2025) provides insight into the rapid growth and security challenges associated with enterprise adoption of AI/ML technologies. "Enterprise AI adoption has skyrocketed over the past year, with a staggering 536.5 billion transactions from AI/ML applications observed in the Zscaler cloud—a nearly 40x surge year-over-year and 60% of all AI/ML transactions were blocked by organizations" (pg. 12 ZTL2025)




" Numerous AI/ML tools have been flagged for data loss prevention (DLP) violations in the Zscaler cloud. These violations represent instances where sensitive enterprise data—such as financial data, PII, source code, and medical data—was intended to be sent to an AI application, and that transaction was blocked by Zscaler policy. Data loss would have occurred in these AI apps without Zscaler's DLP enforcement. (pg. 13 ZTL2025)" This research identifies how AI/ML is enabling more enterprise data to be exposed through applications and there is a need to combat the losses with a zero-trust framework, which also uses artificial intelligence.

**Benefits of SD-WAN Subscription based technologies**

According to Gartner, “by 2027, 70% of network operations personnel will rely on generative AI for Day 2 SD-WAN management, up from less than 5% in early 2024” (GARTSDWAN). This is evidence that the industry is relying on generative AI for state of the art SD-WAN management. In the magic quadrant below from Gartner, these are the top companies that offer a solution for firewall, IDS/IPS, URL/content filtering anti-malware, and much more. They also include orchestrator features in their software that can help with network configuration, management, and troubleshooting. This is an advantage compared to managing a network in house without any additional SaaS from vendors.




“Technologies such as SD-WAN have emerged to help accelerate high-priority traffic, but SD-WAN technologies fail to eliminate the ability of attackers to move freely throughout corporate networks. In fact, by extending the enterprise’s trusted network to branches and clouds, many SD-WAN solutions make the risks associated with lateral movement even higher”. (SDWANZT)

**Ansible**

“Ansible is an open-source automation platform that simplifies network configuration and management by providing a declarative, agentless approach to automate repetitive tasks across diverse network devices and platforms. Its network automation capabilities, detailed in the Ansible documentation (https://docs.ansible.com/ansible/latest/network/index.html), enable consistent management of routers, switches, firewalls, and load balancers from vendors like Cisco, Juniper, Arista, and others” (ANS2025).

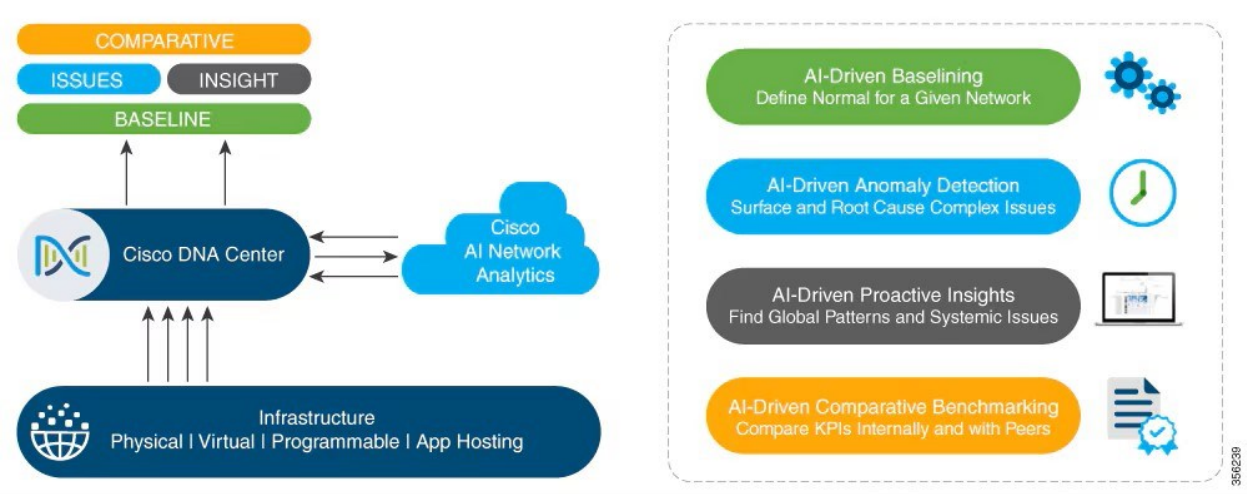
Ansible is very advantageous for AI use cases for AI-drive networking and infrastructure management for AI workloads and integrating insights into network operations. Examples include:

1. Network events that are detected via artificial intelligence anomaly detection can trigger ansible playbooks to remediate issues, like rerouting traffic or isolating compromised devices. An example of this could be use in the Cisco Catalyst SD-WAN, Azure SD-WAN, or AWS SD-WAN.
2. Ansible playbooks can also update systems from AI-generated recommendations from network analyzer tools to adjust configurations dynamically. This is good for network optimization using artificial intelligence or data insights from other integrated tools.
3. Support for modules for managing devices from Cisco, Juniper, Arista, allowing an administrator to create a .yml file playbook to configure networking hardware.
4. Automation of repetitive tasks for updating ACLS, VLANS, which can reduce manual errors. This can work in Cisco and Juniper routers.

The reasons Ansible has been and will continue to be revolutionary in network infrastructure automation is because it supports provisioning multiple machines at once, it integrates with AI tools and platforms, it is integrated with many computer and vendor companies, and it can assist with AI-driven insights for optimizing network performance and security. It can assist in automating tasks in SD-WAN configuration, event-driven responses, and traditional networking in AI driven environments.

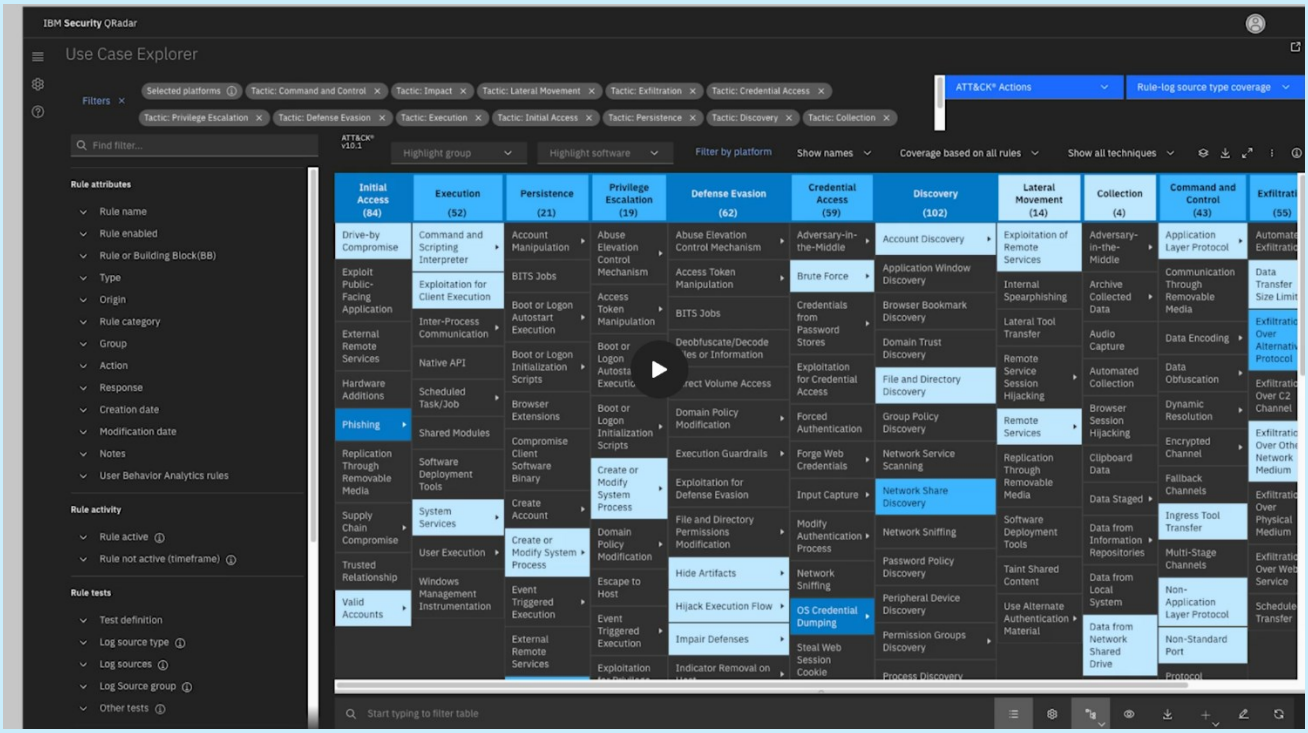
**Cisco AI Network Analytics**

“Cisco AI Network Analytics is an application within Cisco DNA Center that leverages the power of machine learning and machine reasoning to provide accurate insights that are specific to your network deployment, which allows you to quickly troubleshoot issues” (CISCO2025). This application leverages machine learning and creates adaptive baselines for specific networks, while continuing to analyze telemetry data to identify critical issues. This is an advantage of a network analytics tool for security because it reduces false positives, speeds up root-cause analysis, and enable SOC teams to focus on higher priorities, which as a result, can save the company money in the long term. However, a disadvantage of paying for this application depends on the Cisco DNA Advantage licensing and which limits accessibility for companies with older legacy systems or any networks with multi-party vendor hardware environments. However, the benefits for Cisco-centric networks is a great advantage! Below is a screenshot from Cisco’s website showing the flow of data through the Cisco DNA Center.




**IBM QRadar SIEM**

Security Information and Event Management (SIEM) software enable real-time threat detection, advanced analytics and automated response capabilities. One worth noting is the QRadar SIEM by IBM. This is advantageous to the evolution of SIEM systems because of it's enterprise-grade AI features built in to assist automation of monitoring user behavior, network activity, threat intelligence and alerts to reduce noise. It has a feature where for each alert and user or IP address, the GUI will provide the MITRE ATT&CK matrix and tell you what techniques were used. This would not be possible without the assistance of ML and AI. There are over 700 prebuilt integrations that you can use. "QRadar supports compliance with regulations like GDPR and features native integration with open-source SIGMA rules for evolving threats" (IBM2025).

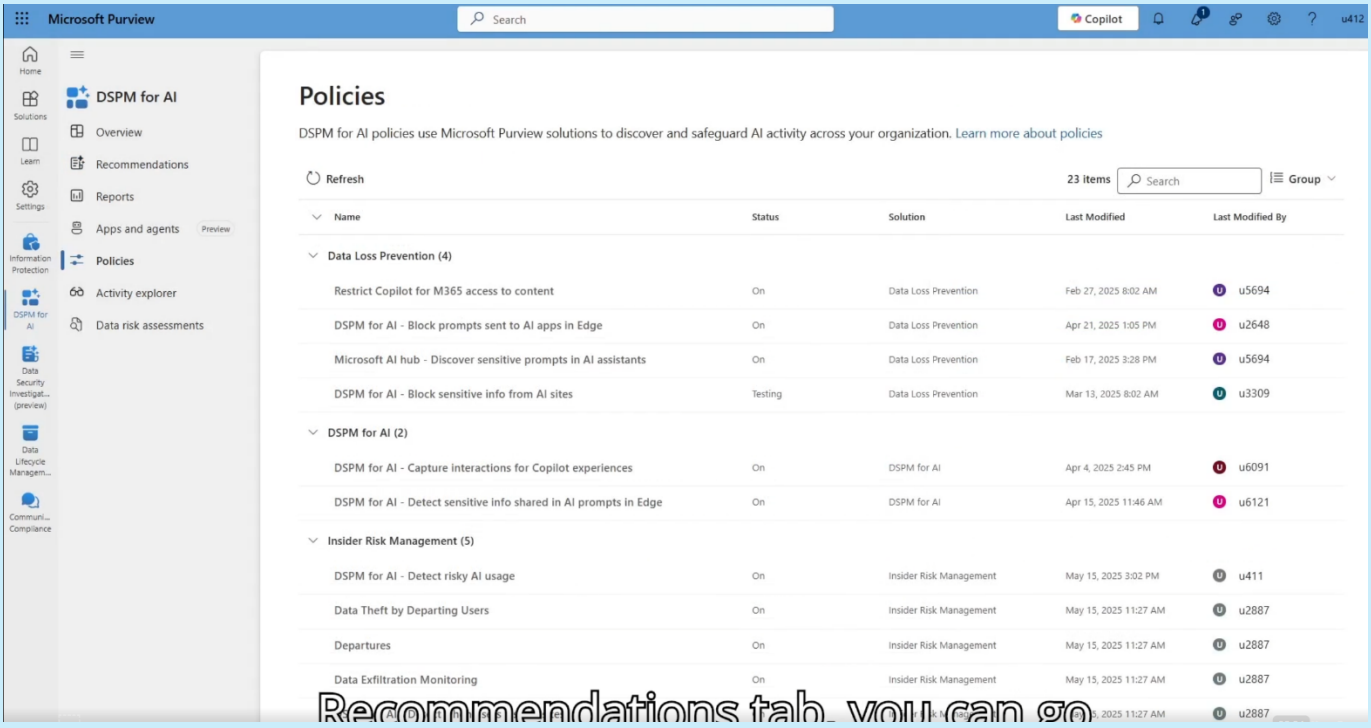


**Microsoft Purview**

"Microsoft Purview Data Security Posture Management (DSPM) for AI from the Microsoft Purview portal provides a central management location to help you quickly secure data for AI apps and proactively monitor AI use. These apps include Copilots, agents, and other AI apps that use third-party large language modules (LLMs)" (DPSM2025). As a network administrator, when your company adopts AI technologies, an advantage of Purview integrating with LLM's such as Copilot, ChatGPT, or other enterprise AI apps, enables the company to take advantage of the following bullet points which I directly sourced from Microsoft's website (DPSM2025).

- Insights and analytics into AI activity in your organization
- Ready-to-use policies to protect data and prevent data loss in AI prompts
- Data risk assessments to identify, remediate, and monitor potential oversharing of data.
- Compliance controls to apply optimal data handling and storing policies

For full functionality though, it requires Microsoft 365 E5 or E5 compliance licenses. Microsoft Purview Data Security Posture Management (DPSM) tool for AI is a suite of *different* tools to monitor, secure, and govern AI interactions, leveraging AI-driven analytics and preconfigured policies to address risks. Below is a screenshot showing what the policies page looks like.

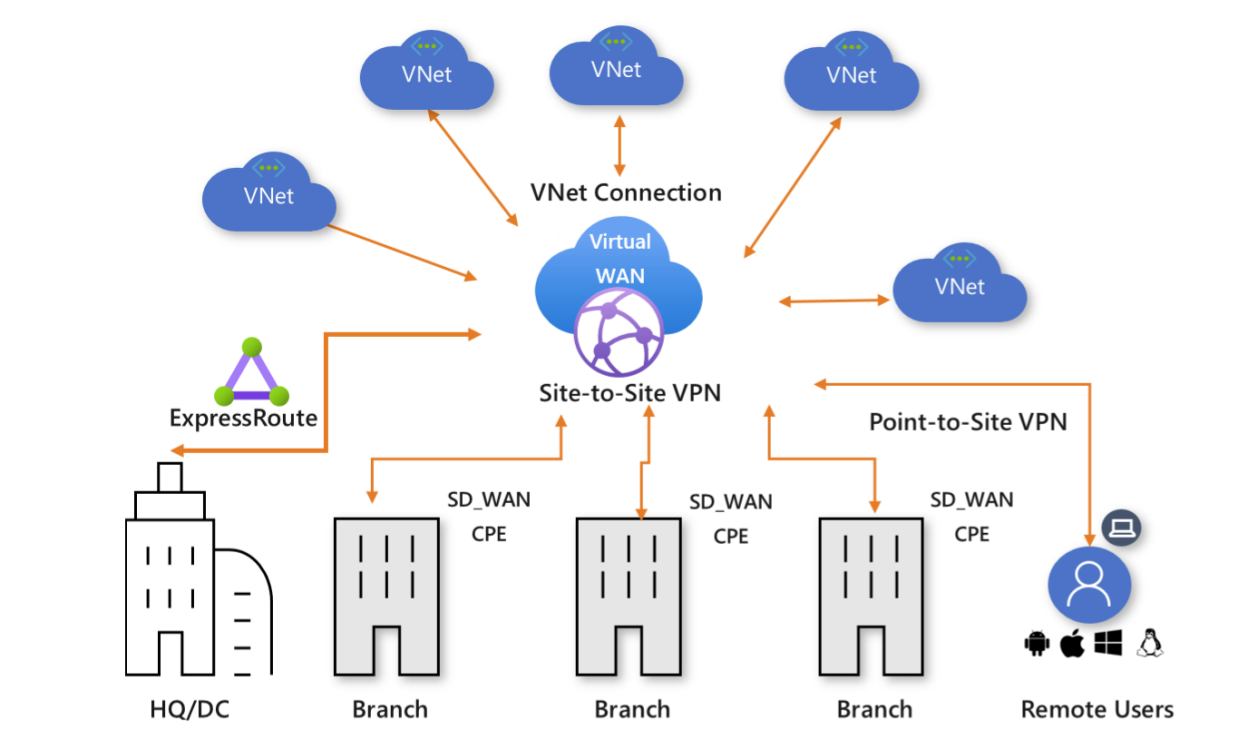



**Azure Virtual WAN**

"Azure Virtual WAN is a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface" (MICRO-SDWAN2025). This cloud based SD-WAN that has partnerships with Cisco, VMware, and Versa Networks, which enables AI driven traffic routing. The platform uses Fortnit for AI-driven threat protection and automation tools from Cisco Cloud OnRamp. It is beneficial for BGP failover reliability,

however a disadvantage is its limited proprietary features and network virtual appliances (NVAs). Other benefits from this list I sourced directly from Microsoft's website (MICRO-SDWAN2025):

- Branch connectivity (via connectivity automation from Virtual WAN Partner devices such as SD-WAN or VPN CPE).
- Site-to-site VPN connectivity.
- Remote user VPN connectivity (point-to-site).
- Private connectivity (ExpressRoute).
- Intra-cloud connectivity (transitive connectivity for virtual networks).
- VPN ExpressRoute inter-connectivity.
- Routing, Azure Firewall, and encryption for private connectivity.




Disadvantages of Azure Virtual WAN could be pricing.

**Amazon Web Services AWS Cloud WAN**

"AWS Cloud WAN is a managed wide-area networking (WAN) service that you can use to build, manage, and monitor a unified global network that connects resources running across your cloud and on-premises environments. It provides a central dashboard from which you can connect on-premises branch offices, data centers, and Amazon Virtual Private Clouds (VPCs) across the AWS global network" (AWSCLOUD2025). Amazon's SD-WAN is primarily supported by partner data centers and ISPs. Benefits of AWS Cloud WAN are its global, AI-driven path

selection, policy-drive automation with APIs, and partnered AI companies and AWS network firewall.

Disadvantages of AWS Cloud WAN could be their costs. Costs can be found here and is on a per hour basis so it can get really expensive: https://aws.amazon.com/cloud-wan/pricing/ . Pricing factors depend on core network edge connection points, data processing, core network edge attachments, data transfer charges, and peering connections. Another disadvantage is VPN throughput is limited to 5Gps and rely on third party vendor artificial intelligence.

**Concluding Remarks**

In conclusion, the standards for a secure and safe network are changing due to modern technology and advancements in publicly available AI applications and LLMs. There are many more advantages to integrating the use of artificial intelligence, machine learning, and cloud service provider applications in network configuration management, IDS/IPS, SD-WAN, automation, SASE networks, SD-WAN, and in implementing a zero-trust architecture. While it can be complex to migrate and adopt the use of these new technologies coming out, it will pay off in the long term by decreasing the attack surface and proactively combating sophisticated cyber threats. Tools like Ansible and Purview help streamline network automation and data security, while platforms like Azure Virtual WAN and AWS Cloud WAN leverage AI for optimized routing. As the cybersecurity landscape evolves, adopting zero trust architecture frameworks with enhanced AI capabilities and adopting SASE architectures will be critical for distributed networks. There are also many advantages to leverage the strengths of AI while mitigating against vulnerabilities and attackers by using tools such as Purview, SD-WANs, vendor specific analytics applications, and AI driven SIEMs.

**References**


1. Zscaler, Implementing the NIST Zero Trust Architecture with Zscaler, 2022 (ZTA2022) https://www.zscaler.com/resources/white-papers/zscaler-implementing-NIST-zero-trust-architecture.pdf

2. Zscaler, “ThreatLabz 2025_AI Security Report “ (ZTL2025) https://www.zscaler.com/resources/industry-reports/threatlabz-ai-security-report-2025.pdf

3. Zscaler, “Rethinking Enterprise SD-WAN with Zero Trust”, 2024, (SDWANZT) https://www.zscaler.com/resources/white-papers/rethink-enterprise-sd-wan-security-with-zero-trust.pdf

4. Zscaler, “Zscaler ThreatLabz 2023 Ransomware Report”, 2023, (ZTLBRR) https://www.zscaler.com/resources/industry-reports/2023-threatlabz-ransomware-report.pdf

5. IEEE, “Machine Learning and the Secure Access Service Edge”, Steven A. Wright, Achyuth Sathyagiri, Ravish Tayal, 2023, (MLSASE) https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10487274

6. IEEE, “Anomaly Based Intrusion Detection using Large Language Models”, Zineb Maasaoui, Mheni Merzouki, Abdella Battou, Ahmed lbath, 2023, (ABIDLLM) https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10912623

7. Amazon Web Services, “What is Amazon GuardDuty?”, 2025, (AWSGD) https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html

8. Office of Management and Budget, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles” 2022, (USGCPT) https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

9. Jacob Serpa, “How to Cut IT Cost and Complexity with a Zero Trust Architecture”, 2022, (ITCOSTZTA) https://www.zscaler.com/blogs/product-insights/how-cut-it-cost-and-complexity-zero-trust-architecture

10. Jonathan Forest, Karen Brown, Nauman Raja, “Magic Quadrant for SD-WAN”, 2024, (GARTSDWAN) https://global.fortinet.com/lp-en-ap-2024-gartner-mq-sdwan?lsci=701Hr000002MO7ZIAW

11. Alan Weissberger, “Fortinet and Palo Alto Networks are leaders in Gartner Magic Quadrant for Network Firewalls”, 2023, (FORTPALO)

https://techblog.comsoc.org/2023/01/15/fortinet-and-palo-alto-networks-are-leaders-in-gartner-magic-quadrant-for-network-firewalls/

12. “The History of Firewalls | Who Invented the Firewall?”, 2024, (PALONGFW), https://www.paloaltonetworks.com/cyberpedia/history-of-firewalls

13. “Ansible for Network Automation”, 2025, (ANS2025), https://docs.ansible.com/ansible/latest/network/index.html

14. “Learn about Data Security Posture Management (DSPM) for AI”, 2025, (DPSM2025), https://learn.microsoft.com/en-us/purview/dspm-for-ai

15. “NIST Trustworthy and Responsible AI NIST AI 100-2e2023 Adversarial Machine Learning A Taxonomy and Terminology of Attacks and Mitigations”, 2023, (NIST-TAX2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf

16. “Chapter: Cisco AI Network Analytics Overview”, 2025, (CISCO2025), https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-assurance/2-3-5/b_cisco_dna_assurance_2_3_5_ug/b_cisco_dna_assurance_2_3_3_ug_chapter_010.html

17. “Empowering today’s modern SOC with enterprise-grade AI”, 2025, (IBM2025), https://www.ibm.com/products/qradar-siem#experience

18. “What is Azure Virtual WAN?”, 2025, (MICRO-SDWAN2025), https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

19. “What is AWS Cloud WAN?”, 2025, (AWSCLOUD2025), https://docs.aws.amazon.com/network-manager/latest/cloudwan/what-is-cloudwan.html