COMPUGEN

Innovate. Inspire. Impact.

How AI Supports the Future of Enterprise Networking

How AI Supports the Future of Enterprise Networking

The future of the modern enterprise network is AI-driven, efficient, agile, and secure.

We're in the age of AI-powered everything — but what exactly is this technology's role in modern networking?

This guide explores how AI enables a modern workspace, enhances data security, and supports hybrid IT. Plus, you'll learn what AI technologies you need and how to ensure a successful implementation.

What is AI in Networking, and What are the Benefits?

Artificial intelligence (AI) is software that can simulate intelligent decision-making in computers, performing tasks on par with a human expert. It plays an increasingly important role in managing complex and distributed IT networks and addressing the proliferation of users, data, and devices.

AI-driven network technology improves troubleshooting, accelerates issue resolution, and provides remediation guidance. Enterprises can automate maintenance and repair tasks to minimize errors, reduce costs, and ensure timely responses.

Meanwhile, AI software can collect and analyze vast amounts of data to help IT teams respond to problems promptly and improve the user experience. It can also use predictive analytics to provide insights, helping IT teams address issues before they cause downtime and delays that can lead to loss of business or damage your reputation.

Moreover, AI-driven tools provide granular and timely security insights. Organizations can improve threat mitigation and response throughout their networks to prevent data loss, breaches, or compliance violations.

AI can benefit many aspects of enterprise networking — minimizing the challenge of talent shortages, lowering operating costs, and performing tasks that are simply not feasible to do manually. In particular, it's essential for handling hot topics like modern workspace, cybersecurity, and hybrid IT. Let's look at how AI supports these specific use cases.

AI in Networking Facilities Hybrid Work and Modern Workspace

A modern workspace provides employees with the flexibility and accessibility to work from anywhere and at any time to optimize productivity and perform at their best. The hybrid work environment helps reduce costs while enhancing remote collaboration and in-person interactions.

But the approach also requires a more complex IT infrastructure to support seamless workflows and communications. AI helps facilitate hybrid work, deliver a high-quality employee experience while allowing organizations to improve cost efficiency:

Real-Time Insights

AI software can collect and analyze real-time data to generate insights about employee activities and productivity no matter where they are. Supervisors can provide guidance, address issues promptly, and make real-time decisions to optimize efficiency and productivity without being in the same room as the employees.

Process Automation

Automation helps reduce the number of manual and repetitive tasks so employees can focus on their core competence and maximize their productivity. For example, AI-driven chatbots and customer service bots can handle routine inquiries so human agents can spend their time resolving complex issues and delivering a better customer experience.

Meanwhile, automating HR processes help deliver a consistent and seamless employee experience no matter where the teams are. You can streamline recruitment, onboarding, training, etc., to ensure employees get the support they need when they need it and become productive as quickly as possible.

Employee Communications

AI can analyze data to identify team collaboration patterns to minimize friction and enhance productivity. The technology can also support wireless network management for fast and reliable communication. For example, AI-enhanced radio resource management can analyze network behaviors and usage trends to set the ideal configurations as network conditions change.

Security and Compliance

Remote working increases an organization's attack surface, making it harder to detect suspicious activities and enforce a data governance policy. AI bots can help analyze network and employee activities in real-time to prevent unauthorized access, data breaches, or violation of data security guidelines.

AI in Networking Supports Cybersecurity

Cybersecurity is a significant concern for companies of any size. Timely detection, proactive intervention, accurate analytics, and immediate incident response are critical in preventing attacks that could lead to costly breaches, downtime, loss of business, and compliance violations.

But the proliferation of devices and the growing size of activity logs have made it virtually impossible for even the best professionals to defend a network. Here's how AI can help:

SecOps

SecOps combines security and IT operations to identify security threats in real-time and enable immediate incident response. AI software can combine data from multiple sources (e.g., intrusion detection system), generate timely insights, initiate responses to mitigate DDoS attacks, filter phishing attempts, and perform endpoint classification.

Additionally, AI-driven network security tools use techniques like behavioral analytics to automatically identify anomalous network traffic, inspect questionable network flows, and deny suspicious traffic. The analytics capabilities are superior to rule-based systems because they can detect zero-day attacks and stealthy threats that can evade traditional anti-virus software.

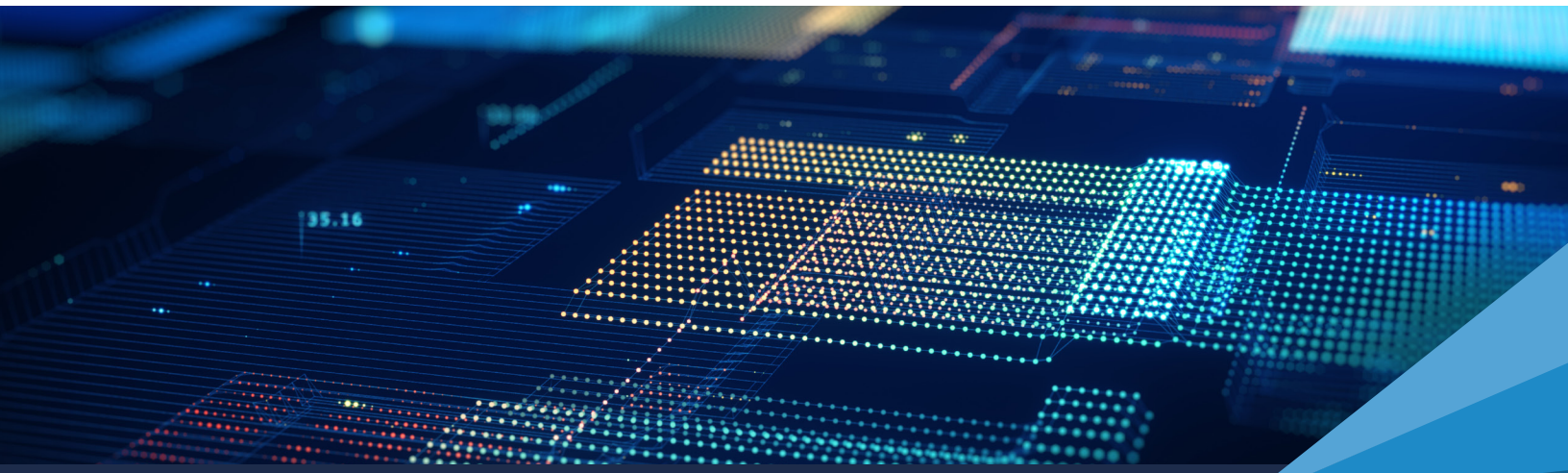
Log Analysis

With increased network activities come massive amounts of log data, which IT teams must analyze and understand to inform timely and accurate decision-making. AI and machine learning (ML) technologies provide advanced event correlation and identify hidden patterns that could indicate potential attacks. The insights can help security teams focus resources on initiating targeted responses.

Endpoint Protection

Do you have a complete inventory of every device connected to your network and know that every one of them is properly configured to comply with your network policy? If the answer isn't a definitive yes, bad actors could find weak points to breach your network. Yet, manually tracking down each endpoint device is almost impossible in today's enterprise environment.

AI security tools can help reduce human errors and oversight by automatically recognizing all devices connected to a network and applying the appropriate policy with minimal human interventions. You can also gain granular visibility into your network and device ecosystem to monitor user behaviors and support a zero-trust network environment.



AI in Networking Optimizes Hybrid IT

More organizations are implementing a hybrid cloud strategy to leverage public cloud platforms' scalability, flexibility, and cost-saving benefits while maintaining control over their data security with on-premises infrastructures.

However, manually configuring and maintaining a hybrid cloud is complex — daunting even for organizations with large IT teams. AI networking tools can help streamline hybrid IT management while ensuring that all the moving pieces are working together to maximize your investment:

Resource Utilization

AI-driven intelligent resource allocation capabilities can analyze workloads, performance data and requirements, resource availability, costs, and user patterns to allocate workload efficiently across on-premises infrastructure and cloud services. You can minimize costs, optimize performance, and scale your infrastructure up or down on a dime without any manual intervention.

Predictive Analytics

AI algorithms can analyze historical data and patterns to predict future resource utilization, system failures, and performance issues. The insights can help you forecast capacity and proactively address problems before they impact your networks and business operations. AI can also forecast demand for cloud resources to help you optimize provisioning.

Network Monitoring

It's challenging (if not impossible) to wrap your head around all the activities in a complex hybrid environment. AI-driven network tools can correlate and analyze metrics, logs, and events from on-premises and public cloud environments to identify anomalies, detect performance bottlenecks, and predict failures. IT teams can quickly isolate, prioritize, and resolve issues to improve network reliability and increase uptime.

Intelligent Automation

AI can automate various routine IT tasks in managing a hybrid environment to improve efficiency, reduce labor costs, and minimize errors. These include resource provisioning and de-provisioning, patch management, back and recovery, etc. The automation capabilities help improve network performance and reliability while freeing IT teams to focus on high-value tasks and strategic initiatives.

Key AI Capabilities for Managing an Enterprise Network

Here are the essential AI and ML technologies to support effective network management:

- Network automation: Automate the deployment and management of network policies, integrate a zero-trust architecture to strengthen network security, and identify and classify all devices connected to the network for complete endpoint visibility.

- AI and ML models: Benchmark network health using historical data and generate insights from long-term variations to compare performance across the organization and against industry trends.

- Network telemetry: Collect data through a network controller and deliver insights via management dashboards to identify anomalies, eliminate false positives, and suggest remediation actions.

- Machine reasoning (MR): Use acquired knowledge to navigate potential solutions toward an optimal outcome. The capability builds on conclusions from ML functions, analyzes possible causes, and recommends improvement options.

- Predictive analytics: Anticipate events such as failures or performance issues using a model trained with historical data. You can also use mid- and long-term predictions to model your network for degradation or outage prevention.

Besides these technologies, you need a robust AI strategy to support successful implementation. AI outputs are only as good as the data you put into the program. As such, the foundation of any successful AI implementation is vast amounts of high-quality data the model can ingest and learn from. Your datasets should be complete and accurate and include data from diverse sources.

Meanwhile, AI can't learn on its own or fix your data. You must provide the software with labeled information based on domain-specific knowledge. Well-organized and accurate metadata is critical for training AI models to ensure they can process subsequent input correctly. After building the capability to segment and classify data, you must feed the metadata into an AI program where supervised or unsupervised ML technology and neural networks analyze the data and generate insights.

But how do you make the insights actionable for various stakeholders with different needs and responsibilities? A virtual network assistant uses collaborative filtering to sort through large datasets, correlate the information, and generate targeted recommendations. It can answer user queries or address specific problems via an intuitive interface.

4 Steps to Implementing Your Next-Level Enterprise Network

Building an efficient, agile, and secure network with the latest AI technologies can be challenging for many enterprises because of the numerous moving parts. Companies need specialized knowledge in multiple domains and address various concerns, from security and performance to employee experience, for a successful implementation.

Yet, not taking action to adopt the technology is no longer an option — market demands and business growth are stretching legacy systems and networks beyond their capabilities. That's why more organizations partner with industry experts like CSI to prepare their networks for the future.

We follow a 4-step process to build a robust network from the ground up and maximize your IT investment:

1. Simplify: Our intent-based networking approach translates policies into action to ensure consistency across the entire physical and virtual infrastructure without extraneous or conflicting elements.

2. Centralize: Create an intelligent fabric to cost-effectively connect all your locations, streamline policy control, achieve granular monitoring, improve network visibility, and integrate IT workflows.

3. Automate: Support the agility of cloud computing with fully managed connectivity to continuously monitor and adjust network performance against desired business outcomes.

4. Protect and respond: Ensure ongoing security and business resiliency by containing a security incident and preventing the impact from laterally expanding to other areas of the organization.

Moreover, we analyze your total network consumption and utilization for voice, video, data, and business-critical applications. Then, we use the insights to shape, prioritize, and direct traffic to support ongoing optimization and improvement. Meanwhile, our software-defined network architecture puts the power into your hand by giving you complete visibility to tune and customize performance at the click of a mouse.

CSI's enterprise networking services set a solid foundation to support your technology requirements — now and in the future. Learn more about our capabilities and get in touch to see how we can take your network to the next level.