Get smart with networks and security

A new era of networks and security

A new era of networks and security.

New AI, GenAI and machine-learning tools are greatly improving network and security management, but business strategy is key to using them effectively.

The AI and GenAI are grabbing the world's attention in areas like self-driving cars and the authentication of priceless artworks.

They're also working behind the scenes to modernize and strengthen networks and security.

How did this come about?

A growing reliance on digital infrastructure means more data traffic, and more complex data traffic. Then there's the widespread distribution of data across locations and systems. Many organizations are adopting software as a service while migrating at least some of their data and applications to the cloud and rolling out edge-computing services.

Add it all up, and you have an environment that's nearly impossible for humans to manage by themselves. Traditional network management and security measures are inadequate, but advanced AI and machine-learning tools can fill the gaps.

Contents

AI and machine learning in action

Even before the headline-grabbing era of GenAI, AI and machine learning had been used for some time in network and security management to carry out activities like pattern detection and the deep analysis of historical data.

The latest iterations of these tools can detect and respond to security breaches or network incidents even faster and more accurately.

In security, AI-powered threat detection and response is steadily improving the efficiency of attack mitigation, while machine learning plays a key role in predictive security analytics by forecasting vulnerabilities and optimizing network performance with little to no manual intervention.

These tools might also adapt a user's network access dynamically based on their changing attributes. If they are signing in from their home office, for example, it's a low-risk environment, but if they're in an airport connected to public Wi-Fi, their threat profile should be raised.

And, in network management, an AI tool can identify performance issues through techniques like anomaly detection and predictive analysis, including predictive capacity-planning. The next step is formulating – and even fully automating – a response, such as dynamically adjusting the prioritization of applications on a network.

Most of these changes still need human approval. For example, an AI tool might see social media traffic rising sharply on your network and ask for higher network prioritization for that traffic. However, the human network team will know social media should not be prioritized over enterprise resource planning or customer relationship management systems on your network, so the change will not be implemented.

Adding GenAI into the mix

GenAI is a key development in autonomous networks and security.

It supports and extends the capabilities of AI and machine learning by excelling in predictive modeling, threat simulations and generating dynamic responses to cyberthreats.

For instance, GenAI tools can simulate security threats on your network by creating content like phishing emails, just as cybercriminals would do, or generating realistic-looking traffic patterns that signify an attack. This means you can train your employees and machine-learning models to identify new threats in a safe, simulated environment, and avert potential breaches in a real one.

The application of GenAI in networking is still emerging but includes using the technology – rather than a person – to make or suggest network configuration changes.

A machine-learning model can detect and identify a certain event, and a GenAI tool can then suggest a configuration change or update to your IT team. If they approve it, it can be implemented manually or automatically.

These proposed changes can also be simulated in a digital twin of your network before being implemented, to avoid unforeseen effects.

It's important to determine the degree of governance to apply throughout this process, particularly in the context of automated implementations of changes suggested by GenAI (that is, autonomous operations). You need to consider your organization's risk appetite for making such adjustments without the gatekeeping offered by traditional change control.

The convergence of networks and security

Network and security functions have become more converged, and the technology is following a similar pattern.

The ability of these technologies to respond autonomously to security incidents, particularly related to user actions, will keep improving. So will the quality of network service as dynamic configuration changes become smarter and more focused.

Having a unified view of the threat landscape as well as your network performance supports converged actions like automating the response to a security incident through a network policy change.

It also improves your organization's ability to evaluate the risk or impact of a breach on your entire security and network landscape. What if there's a breach in this location by a user with this level of access? Which systems will be affected, and how? Would the firewall mitigate this threat? You can model the impact more efficiently in a converged network and security environment that's equipped with AI and machine-language tools.

Should you believe the hype?

As powerful and efficient as these AI and machine-learning tools already are, their effectiveness can be overstated. This is especially true in complex environments where humans still have to verify the accuracy and relevance of their recommendations.

Even these advanced tools cannot autonomously detect and prevent every possible threat. They can do far more than a human employee – faster and more accurately – but they are not infallible. An AI tool trained on historical data may be unable to recognize a novel type of threat.

And GenAI, with all its potential, comes with data privacy, accuracy and ethical concerns that must be carefully managed.

The decision-makers in your organization should therefore discern between the true potential of these technologies and the overhyped promises. They also need to understand the risks arising from incorrect responses from AI tools or machine-learning models.

Implementing these smart tools does not negate the need for highly skilled employees in your security and network teams. Instead, they help these employees to be far more effective at their jobs – especially in making decisions and weighing up options while evaluating the high-priority network and security issues identified by the tools.

These employees will need a deep understanding of your business and the context in which certain decisions are to be made so they can train and improve the accuracy of your AI and machine-learning tools over time.

The central role of data, governance and compliance

Using AI and machine learning to improve your network and security has its benefits, but you will need to address issues relating to data quality, data privacy, governance and the accuracy of decisions based on these technologies.

The ability of these technologies to respond autonomously to security incidents, particularly related to user actions, will keep improving. So will the quality of network service as dynamic configuration changes become smarter and more focused.

Having a unified view of the threat landscape as well as your network performance supports converged actions like automating the response to a security incident through a network policy change.

It also improves your organization's ability to evaluate the risk or impact of a breach on your entire security and network landscape. What if there's a breach in this location by a user with this level of access? Which systems will be affected, and how? Would the firewall mitigate this threat? You can model the impact more efficiently in a converged network and security environment that's equipped with AI and machine-language tools.

Weigh up the risks and rewards

Let's say you want to use AI to automate a response to a security or network performance incident.
Which governance framework will be used to decide the action to be taken? And can the decision be made safely without human oversight?

Or, what if a false-positive alert results in a sweeping change to your security and network environment that brings your business activities to a halt? What would the impact on your organization be, and would it outweigh the risk of actual threats going undetected?

Get your data house in order

Getting your data house in order raises even more questions. What data are you using to train your AI and GenAI models? Is it accurate and complete? How often will it have to be refreshed so you can keep training and improving your models?

Data silos aren't helpful in this environment: to train a GenAI model, you need constant access to high-quality, clearly labeled and consistently formatted data across your business. Organizing and cleaning up that data is not a trivial undertaking. A large organization with many business units might have many datasets that can be used to train a model, but if they're stored in separate locations and labeled in different ways, they won't be of much use.

Understand the compliance context

Compliance is central to this effort, too. Your data might contain personally identifiable information about your employees or customers. So, depending on the context, the training data might have to be scrubbed first so you don't risk breaching regional or national data-privacy laws such as the European Union's "right to be forgotten" legislation.

The rigidity of your regulatory and compliance environment will depend on your industry. For example, if you're in the financial services sector in Europe, you'll need a high level of traceability, accountability and auditability – but running security and network decisions through an AI model that operates much like a black box may make that difficult.

Scaling and staffing are also key challenges

You'd expect your AI and GenAI tools to adapt seamlessly to changing demand as your business grows – but scaling these projects is not that easy.

Budgeting for your newly AI-enabled network and security environment – and finding the ROI – may quickly become trickier than you had expected.

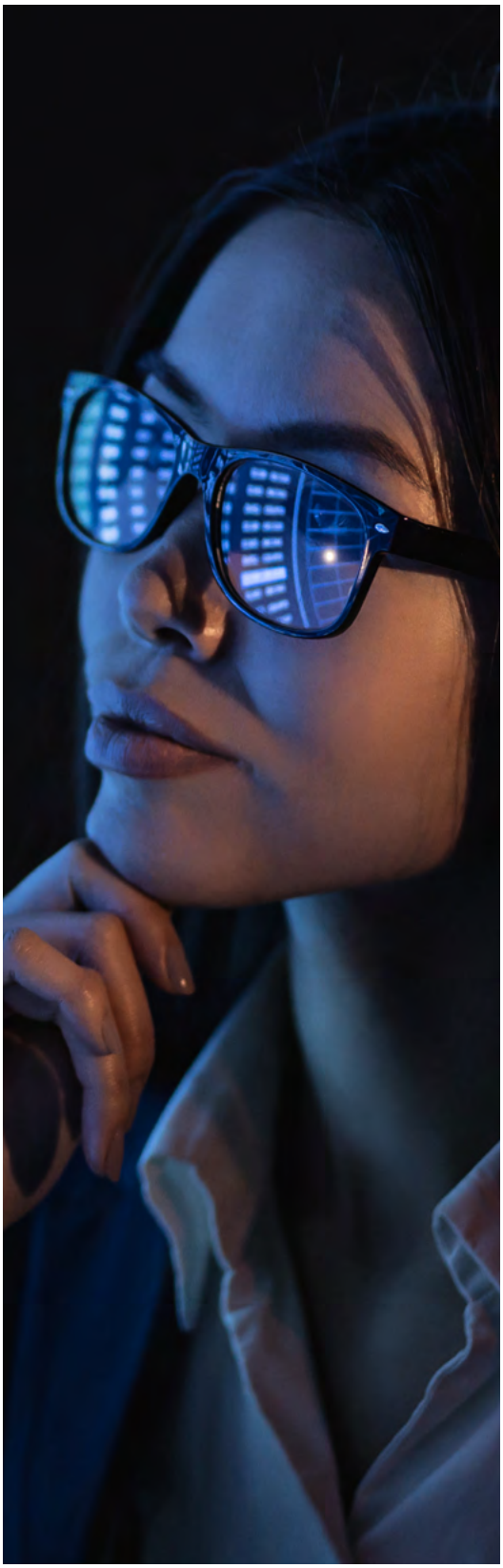
It takes a lot of computing to power to train AI and GenAI models, and the resources required can be expensive to buy or rent. When you're using these tools in production and starting to scale up, the cost of queries or prompts submitted to the model can rise quickly too.

Your security and network teams need AI and machine-learning skills to implement these technologies successfully, and in line with regulations and ethical boundaries.

Depending on how you use these technologies, you might also need data scientists, data engineers, platform engineers and experts in advanced computing to work alongside your network and security operators. They bring the skills needed to monitor the output of your GenAI tools and make sure there are no hallucinations (false information presented as fact) or drift (where the generated output gradually deviates from the intended or desired characteristics over time).

All these skills are in demand, and appointing more network operators and security operations center staff will address your needs only partway.

Can you divert some of your current employees into this space? What will the impact be on the rest of your organization? And, if you bring in experts from outside your organization, what will it cost to retain them in a highly competitive market?



A strategy for success

Considering the expense and complexity involved, buying AI, GenAI and machine-learning tools just for the sake of acquiring new technology for your organization would be a mistake.

Before you invest in a technology solution, you need to know which business problems you hope to solve with it, and what the ROI will be.

Start by determining your organization's vision, long-term strategy and risk appetite. Then consider the data management strategy and skills you'll need.

Draw up a detailed roadmap for your network and security environment – and remember that it's not a finite plan.

You'll have to keep checking the output of your AI and GenAI models and retrain or update them to keep them working as intended. Your employees will also need regular training if they are to use these tools to their full potential.

Work with the experts

So, what's the fastest, most reliable and most cost-effective way to bring AI, GenAI and machine-learning tools into your organization as part of your long-term business strategy?

One effective approach is to bring in external expertise rather than making a significant investment in in-house development.

This is where strategic partnerships with expert vendors and managed service providers like NTT DATA and Palo Alto Networks make a lot of sense.

We're collaborating closely on using AI and machine learning to improve our networking and security solutions. The security tools provided by Palo Alto Networks, like Prisma SASE and Cortex XSOAR, are best in class, while NTT DATA adds value throughout the technology lifecycle with solutions that cover cloud, network, security and business processes.

NTT DATA's AI-powered network platform, SPEKTRA, integrates with Palo Alto Networks solutions to use AI and automation in security for faster threat responses, better detection and response times, and insights into vulnerabilities for proactive defense.

In this way, we help you devise the right strategy to create value from your IT environment while keeping your data and applications secure.

And, because of NTT DATA's global scale, with a footprint in more than 50 countries, we can attract and retain scarce AI, GenAI and machine-learning talent, to the benefit of our clients. Our 7,500+ security specialists can even train your teams in turn.

Take the next step

It's time to separate the hype from the reality when it comes to using AI, GenAI and machine learning in networking and security.

To change the way you do business, think about what to do differently, better and smarter – then work with NTT DATA and Palo Alto Networks to make it happen.

Sign up for a live demo of our SPEKTRA network platform.

List of abbreviations

AI	artificial intelligence
GenAI	generative artificial intelligence
IT	information technology
ROI	return on investment
SASE	secure access service edge


NTT DATA