Brochure

Why zero trust networks are essential in the age of AI

Get started →

Connected enterprises are using their networks to energize AI—providing the high-capacity, low-latency, and reliable connectivity AI needs to unlock efficiencies. But adopting AI comes with security risks. In fact, the entire relationship between AI and cybersecurity and cyberattacks is an interesting one.

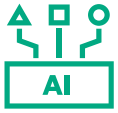
On one side, cybercriminals are targeting AI and machine learning models, seeking to poison AI training data, steal sensitive information, or find model vulnerabilities to exploit. They're also using AI-powered tools themselves to carry out more sophisticated hacking operations—from automating the discovery of vulnerabilities to amplifying the scale and intensity of DDoS attacks, and tailoring phishing campaigns with unprecedented precision.

On the other side, the cybersecurity industry and IT teams are defending against these threats using zero trust security—and are harnessing the power of AI to strengthen their efforts.

Examples of AI-assisted attacks

AI and password cracking

Cybercriminals can use machine learning and AI to crack passwords more efficiently, sifting through massive collections of passwords rapidly and creating sophisticated algorithms to guess your password with alarming accuracy.



AI-assisted phishing

Phishing attempts used to be relatively easy to identify, often through grammatical errors and misspellings. However, AI has enhanced cybercriminals' capabilities to produce convincingly articulated, well-composed content. AI technologies can adeptly mimic the tone, language, and style of legitimate emails, and customize them with greater precision using publicly available data.

Deep fakes and impersonation

Within this genre of cyberattack, there is a specific scam called vishing (similar to phishing but used over the phone). Criminals use AI to mimic the voice of someone you trust, like a coworker or family member. They do this by feeding AI recordings of the person's voice. The AI then creates new speech that sounds just like them. With enough voice data, AI can convincingly impersonate almost anyone.

Examples of attacks on AI models and data

Adversarial machine learning attack

Tricks AI models by altering input data. Attackers can subtly alter visuals or text to misclassify or forecast, potentially damaging an AI systems' trustworthiness.

Data poisoning attack

Inserts harmful or misleading data into training datasets to corrupt learning, resulting in biased or underperforming models that can cause harm.

Model inversion attacks

Reverse-engineers AI models to steal sensitive data. Attackers use model outputs to infer sensitive training data, posing privacy risks and potential breaches.

Exploratory attack

Probes AI systems to learn their underlying workings. Attackers can employ searches or inputs to find vulnerabilities, model behavior, or proprietary information for subsequent assaults.

Resource exhaustion attack

Overloads AI systems with requests or inputs to degrade performance or create downtime.

Protecting AI systems and workloads with zero trust security

So how do you defend against these various AI-related attacks and strengthen the protection of your models and workloads?

Zero trust is a security model designed to secure and limit access to AI infrastructure and models and defend against threats that can bypass traditional perimeter defenses. The principles of zero trust are to never assume trust, even for internal users and systems, but to continuously verify and enforce least-privilege access to resources.

Organizations often use many disparate platforms to achieve zero trust, which can complicate maintenance and allow for potential gaps. However, zero trust deployed at the network level can help to reduce many of the risks and complexities.

Organizations need to think about the network as a security solution—a vital part of their overall security ecosystem and the starting point for a comprehensive cybersecurity strategy. Building a security-first network makes it easier for organizations to activate zero trust principles intrinsically at every point of connection.

How zero trust at a network level protects against AI risks

Preventing and detecting AI infrastructure attacks

Unmanaged IoT devices play a key role in generating data used to train AI. But their often limited security capabilities also make them an attractive entry point for attackers looking to target AI data. A comprehensive zero trust framework can accurately identify and profile IoT devices connected to the network, and continuously monitor their behavior for anything suspicious.

Protecting against AI-aided attacks

If an attack originates via an IoT device, network detection and response (NDR) systems can analyze and detect the unusual behavior to raise an alert. Using network access controls, IT teams can define policies that automate network enforcement and response based on threat telemetry data and anomaly detection.

Ensuring role-based access

Zero trust best practices, such as dynamic segmentation, role-based access control, and continuous policy enforcement ensure that users and devices only communicate with destinations and applications consistent with their role, context, and security posture.

For example, if a device is suspected of participating in an attack, network access controls can automatically limit or revoke network access pending further investigation, stopping lateral spread.

Combatting AI threats with AI

With the volume of users, devices, and applications connecting to networks from anywhere today, ensuring secure access for everyone and everything requires extra help. And it's here where IT and security teams are using AI to combat AI risks and enhance their zero trust efforts.

AI-powered networking improves management and security from several perspectives:

- **AI-powered automation** means that there is less manual effort required to configure and manage the network, contributing to a lower risk of vulnerabilities due to misconfigurations or gaps in protection. Additionally, by multiplying human potential with AI, organizations can mitigate risk at scale to improve security and free up teams to create business advantage.
- **AI-powered security solutions** are specifically designed to solve challenges that can only be solved in the network, such as leveraging network telemetry to enable both the security and networking teams to automatically see who and what is on the network, track their behavior for anomalous activity, and deliver near real-time, actionable AI-powered insights to protect the organization without disruption—all key capabilities necessary to ensure effective zero trust implementation.

AI's role in zero trust security for IoT

Here's an example of AI's role in **zero trust security for IoT**.

Challenge	AI solve
Visibility: IoT devices manufactured by specialized vendors may not support standard profiling methods. Some IoT devices use generic hardware and software, making accurate profiling difficult or leading to generic categorizations that complicate policy enforcement. And most visibility solutions rely on bolt-on collectors or software agents, which are challenging to deploy at scale across numerous IoT devices across multiple locations.	**AI-powered device profiling:** Solutions like Client Insights, powered by AI and part of HPE Aruba Central, can deliver deep visibility and accurate profiling, without the need to install physical collectors or software agents. Client Insights leverages native infrastructure telemetry from access points, switches, gateways, and clients to accurately profile a wide variety of clients across the entire wired and wireless infrastructure using machine learning-based classification models.
Continuous monitoring: IoT devices are often configured once and then forgotten about. Without continuous monitoring, unusual or rogue behavior that can indicate compromise or attack can go unnoticed.	**AI-powered behavioral analytics:** AI-powered IoT discovery and classification features can analyze dynamic device attributes—including traffic patterns and behavioral characteristics such as connection state and network residency—to accurately categorize and identify IoT devices. Once an IoT device is identified, AI can establish behavioral baselines for the device, making it easier to spot anomalies.
Anomaly detection: Trivial fluctuations in device behavior can lead to false positives, contributing to alert fatigue and making it more difficult to detect actual security concerns. Yet looking at data at an aggregate view can mask real indicators of attack.	**AI-powered anomaly detection:** When applied to comprehensive telemetry, AI can detect anomalous behaviors with precision and raise alerts for investigation. Network and security teams can augment this AI model-driven approach by specifying alert thresholds and adjusting the sensitivity of detection to align to organizational risk preferences.
Threat response: Opaque automated responses don't provide enough insight into potential threats. And unclear automated actions can lead to unnecessary disruption.	**AI-powered policy optimization:** These tools can accelerate threat response without operational disruption. Look for a solution that follows a consent-based approach: where network and security teams can preview recommended changes before implementation, allowing them to have greater control and the ability to gauge risk versus impact.

A secure-by-design network from HPE

No single vendor or solution can deliver all the AI cyber risk protection an organization needs. However, starting with a network that provides a built-in foundation for zero trust security can make it easier to implement AI security and compliance requirements, while adding protection at critical digital entry points.

HPE's secure-by-design, self-driving network is built on zero trust principles. By providing advanced visibility, insights, centralized policy management, data protection, threat defense, access control, and AI-powered capabilities that enhance protection at scale, HPE turns the network into a security solution that can protect the organization and defend against AI threats.

Branch

Replace legacy firewalls in branch offices and reduce hardware footprint, cost and complexity with HPE Aruba Networking EdgeConnect SD-WAN, including integrated next-generation firewall capabilities.

Campus

Support security, compliance, and connectivity goals with AI-powered visibility, cloud-native network access control, and policy automation delivered through a wired and/or wireless network managed by HPE Aruba Central.

Infuse zero trust principles everywhere with HPE

Data center

Apply policies consistently across both users and workloads and use microsegmentation to reduce the risk exposure associated with east-west traffic patterns—without the requirement of added firewalls—using built-in security capabilities within the HPE Aruba Networking CX10000 switch.

Cloud

Successfully secure work from anywhere with HPE Aruba Networking SSE—cloud-delivered security services that use adaptive trust and continuous monitoring to increase security while optimizing each connection.

Additionally, our HPE Juniper Networking SRX Series Firewalls natively enable a hybrid mesh firewall architecture, providing the infrastructure to operationalize zero trust across the enterprise:

— Unified enforcement helps ensure that zero trust rules are applied consistently, whether traffic is flowing inside a corporate LAN, between data centers, or into the cloud.
— Granular context allows policies to be tied to users, devices, and applications, rather than just IP addresses or subnets.
— Scalable architecture helps ensure that zero trust protections can grow with the business, from a handful of cloud apps to thousands of workloads.

Learn more at

HPE.com/networking

Visit HPE.com

Chat now

a00148343ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com