Introduction: Zero Trust is your answer to AI risk

The concept of Zero Trust is hardly new, but in the new AI era, it's more important than ever. Forrester Research first promoted it years ago, warning organizations that it was time to overhaul the traditional method of granting unfettered access to any user or application once it passed the network perimeter. Instead, every device, user, and network flow should be verified before full access is granted.

Zero Trust began to gain traction as organizations sought to solve the access problems associated with hybrid work and cloud deployments. But now the perimeter is no longer just remote — it's dynamic and operating at machine speed.

AI has made deepfakes not only possible but sophisticated, and LLM-backed phishing attempts can now be created at scale with unprecedented levels of personalization. More concerning, the prospect of frontier AI models that quickly identify vulnerabilities that had evaded human detection for decades makes a breach not only a question of "if, not when," but of how damaging it will be.

Consider the rise of ransomware as a service, through which developers create ransomware and rent it to affiliates to launch attacks. It allows even unskilled hackers to execute advanced attacks. Recently, three of the most prominent ransomware groups — ALPHV/BlackCat, CL0P, and LockBit — all conducted **quadruple extortion attacks**. In these attacks, threat actors not only encrypt and exfiltrate data but also threaten DDoS attacks and contact a victim's customers, partners, employees, and the media to force them to pay a ransom. Generative AI and LLMs are helping to increase the frequency and scale of ransomware attacks by making it easier for individuals with less technical expertise to launch sophisticated campaigns.

Human-led defenses are too slow to keep up with this new reality. Organizations must quickly pivot to a "defense-first" AI strategy. They need to protect every single digital interaction.

Amid this evolving and often confusing cybersecurity landscape, network and security software vendors have rushed in to brand their existing products as AI-enabled or to introduce new products. It has left security teams struggling to keep pace and confused by the purchasing decisions that set the foundation for a shift to a Zero Trust strategy.

This guide is designed to provide security teams with a blueprint for making investments in Zero Trust technology amidst rising AI threats by identifying where to start and outlining the key differentiating factors.