# The evolving landscape of cybersecurity: adapting to new threats



In the contemporary landscape of cybersecurity, the urgency for organisations to evolve their protections against a myriad of threats has never been more paramount. High-profile cyber incidents in recent years have illuminated significant vulnerabilities, prompting experts like Gurucul CEO Saryu Nayyar to emphasise the importance of adapting cybersecurity measures to combat emerging threats. Speaking to BetaNews, Nayyar provided insight into the current state of cybersecurity and the transformative potential of AI and machine learning.

Nayyar's comments were underscored by findings from Gurucul's 2024 Insider Threat Report, which revealed that nearly half of companies surveyed reported a rise in insider attacks. Specifically, 48 percent of organisations experienced more insider threats within the past year, and 51 percent faced six or more significant incidents. These statistics reflect a pressing reality: traditional methods of defence appear increasingly inadequate against sophisticated cyber threats.

To effectively counteract these evolving challenges, Nayyar advocated for the integration of proactive security strategies that leverage advanced technologies. "The challenge isn't just about keeping pace with new threats but ensuring resilience and adaptability for future security," she expressed. AI, in particular, is being harnessed to enhance threat detection through the establishment of behaviour baselines and real-time anomaly detection. This innovative approach involves utilising machine learning models to determine what constitutes normal activity and flagging deviations that could signify potential threats.

Another notable application of AI is in predictive risk scoring, which analyses behaviours across various datasets to assign dynamic risk scores. This method aids security teams by prioritising threats for quicker responses and reducing false positives—thereby allowing teams to focus on the most critical threats rather than becoming overwhelmed by irrelevant alerts.

However, Nayyar also pointed out the dual-edged nature of AI in cybersecurity. As organisations adopt AI to bolster their defences, cybercriminals are similarly leveraging these advanced technologies to enhance their attack strategies. This technological arms race underscores the necessity for continuous innovation in defensive measures, ensuring that security frameworks are adaptable and capable of evolving alongside new threats.

In light of the expanding role of technology in cybersecurity, Nayyar highlighted the potential for governments to play a more significant role in promoting cybersecurity initiatives. She noted ongoing regulatory efforts in the United States and abroad aimed at protecting sensitive information and critical infrastructure. These regulations, including the Federal Information Security Modernization Act (FISMA) and various industry-specific standards, represent an essential framework for organisations to assess their compliance obligations and bolster their security operations accordingly.

Discussing future technologies critical for combatting threats, Nayyar reiterated the significant role of AI and machine learning in detecting and responding to threats in real-time. Additionally, she identified Zero Trust architecture as a pivotal component in enhancing security measures. This approach demands continuous verification of user identities for every access point, irrespective of a user's location, thereby reducing avenues for potentially unauthorised access.

Nayyar’s reflections on the trajectory of recent cyberattacks serve as an important indicator of the challenges ahead. A substantial portion of organisations cite the complexity of their IT environments as a significant factor contributing to security vulnerabilities. According to data from Gurucul’s reports, 39 percent of organisations identified this complexity as a key contributor to the rise in insider attacks. Such insights reveal that a unified approach to cybersecurity—where data integration is paramount—can significantly enhance an organisation’s ability to detect threats and respond effectively.

With the relentless pace of technological advancement and growing sophistication of cyber threats, the consensus is clear: organisations must evolve their strategies alongside these developments. By harnessing next-generation technologies like AI and machine learning, coupled with coherent and unified defensive strategies, organisations can enhance their resilience and agility against both internal and external threats.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://aspioneer.com/saryu-nayyar-setting-benchmarks-in-the-cyber-world-for-others-to-follow/> - Corroborates Saryu Nayyar's role as CEO of Gurucul and her emphasis on the use of AI and machine learning in cybersecurity, particularly in threat detection and reducing false positives.
* <https://aspioneer.com/saryu-nayyar-setting-benchmarks-in-the-cyber-world-for-others-to-follow/> - Supports the use of Gurucul's Next-Generation SIEM (NGSIEM) and User & Entity Behavior Analytics (UEBA) in detecting and responding to cyber threats.
* <https://www.redhat.com/en/blog/4-use-cases-ai-cyber-security> - Explains the use of AI in detecting cybersecurity anomalies and identifying behavior deviations, which aligns with Nayyar's comments on AI in threat detection.
* <https://www.redhat.com/en/blog/4-use-cases-ai-cyber-security> - Discusses AI's role in predicting threats and identifying vulnerabilities, supporting the notion of AI's transformative potential in cybersecurity.
* <https://www.techmagic.co/blog/ai-in-cybersecurity/> - Details AI's application in threat detection, predictive risk scoring, and automated response mechanisms, aligning with Nayyar's insights on AI in cybersecurity.
* <https://www.techmagic.co/blog/ai-in-cybersecurity/> - Highlights the use of AI in user behavior analytics and advanced threat response, which is consistent with Nayyar's advocacy for proactive security strategies.
* <https://gurucul.com/press-releases/gurucul-ceo-saryu-nayyar-named-winner-of-the-top-10-women-in-cybersecurity-for-2021/> - Confirms Saryu Nayyar's leadership and Gurucul's pioneering role in User and Entity Behavior Analytics (UEBA) and other cybersecurity technologies.
* <https://gurucul.com/press-releases/gurucul-ceo-saryu-nayyar-named-winner-of-the-top-10-women-in-cybersecurity-for-2021/> - Supports the integration of AI and machine learning in Gurucul's Unified Security and Risk Analytics platform for threat detection and response.
* <https://aspioneer.com/saryu-nayyar-setting-benchmarks-in-the-cyber-world-for-others-to-follow/> - Addresses the dual-edged nature of AI in cybersecurity, where both defenders and attackers leverage AI, aligning with Nayyar's comments on the technological arms race.
* <https://gurucul.com/press-releases/gurucul-ceo-saryu-nayyar-named-winner-of-the-top-10-women-in-cybersecurity-for-2021/> - Highlights the importance of regulatory efforts and compliance in cybersecurity, such as FISMA, which is mentioned in the context of government roles in promoting cybersecurity.