The Future Of Defense

Cybersecurity Trends and Insights for 2024

AI threats cast a looming shadow as we step into 2024, making proactive cybersecurity strategies increasingly critical to counter both existing and emerging threats. Keeper Security commissioned an independent research agency to survey over 800 IT security leaders around the globe about what's on the cybersecurity horizon.

The attack vectors increasing the fastest

1. Phishing
2. Malware
3. Ransomware
4. Password Attacks
5. Denial of Service (DoS)

95%

of IT leaders say cyber attacks are more sophisticated than ever before

The most serious emerging attack vectors

1. AI-Powered Attacks
2. Deepfake Technology
3. Supply Chain Attacks
4. Cloud Jacking
5. Internet of Things (IoT) Attacks

> As emerging technologies, such as AI, fuel the next wave of cyber threats, a great paradox lies in our ability to implement the very innovations that, if not controlled properly, will radically increase cyber risk. With the cybersecurity tools at our disposal today, we possess the arsenal to mitigate emerging threats - thereby converting this challenge into an opportunity for resilience and fortification of our digital defenses.
>
> **Darren Guccione**
> CEO and Co-founder
> Keeper Security

Evolving threats demand constant adaptation which must remain a top priority for IT leaders. A password manager can mitigate risks by enforcing strong password practices, while privileged access management safeguards an organization's vital assets by controlling and monitoring network access, collectively fortifying defenses and minimizing potential damage in the event of an attack. Integrating these solutions creates a layered security approach that minimizes risk to enhance overall cybersecurity resilience.