Technology Topic Summary

intel ai

Artificial Intelligence (AI) in Cybersecurity

AI-assisted security technologies can help businesses proactively combat evolving cyber threats to protect their operations, innovations, and data.

AI in Cybersecurity at a Glance

Business challenges:

- Enterprises face a rapidly evolving cybersecurity landscape.
- Combating cyber threats at scale is beyond human-only abilities.
- Endpoint devices are the primary entry point for attacks targeting the whole system stack.[1]
- Legacy tools don't provide needed visibility from edge to cloud.

Solutions:

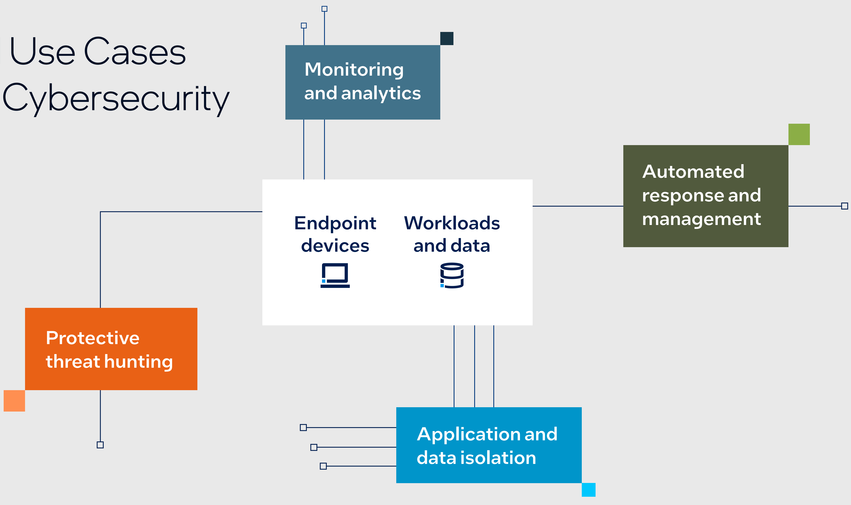
- AI enables autonomous, near-real-time threat detection and response.
- AI in cybersecurity enhances the protection of data, AI models, and physical devices.
- Hardware-based security capabilities can add a layer of defense across the technology stack.

Benefits of AI in Cybersecurity

AI cybersecurity solutions help IT teams combat cyber threats.

- **Improve detection:** Monitor systems and data in near-real time for new and known threat patterns.
- **Automate response:** Preemptively act on threats and attacks using AI analysis of prior solutions.
- **Extend reach:** Enhance existing security solutions with AI-based tools to expand visibility.
- **Reduce risk:** Help reduce data breach risks and costs with AI[2] for defense in depth.

AI Use Cases in Cybersecurity



intel ai

Stay ahead of evolving cyber threats

Find out how at intel.com/ai

1. "What is endpoint security?" IBM, accessed May 31, 2024, ibm.com/think/topics/endpoint-security.
2. "Cost of a Data Breach Report 2024," IBM Security, accessed January 14, 2025, ibm.com/reports/data-breach.

Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.
© Intel Corporation